LA CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

ÓRGANO DE CONTROL INSTITUCIONAL

INFORME DE VISITA DE CONTROL N° 008-2022-OCI/2911-SVC

VISITA DE CONTROL MUNICIPALIDAD PROVINCIAL DE HUARMEY, PROVINCIA DE HUARMEY, REGIÓN ÁNCASH

"USO DEL SISTEMA SIAF EN LA MUNICIPALIDAD PROVINCIAL DE HUARMEY"

PERIODO: DEL 4 AL 10 DE MAYO DE 2022

TOMO I DE I

HUARMEY, 16 DE MAYO DE 2022

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

INFORME DE VISITA DE CONTROL N° 008-2022-OCI/2911-SVC

"USO DEL SISTEMA SIAF EN LA MUNICIPALIDAD PROVINCIAL DE HUARMEY"

ÍNDICE

INFORME DE VISITA DE CONTROL N° 008-2022-OCI/2911-SVC

"USO DEL SISTEMA SIAF EN LA MUNICIPALIDAD PROVINCIAL DE HUARMEY"

I. ORIGEN

El presente informe se emite en mérito a lo dispuesto por el Órgano de Control Institucional de la Municipalidad Provincial de Huarmey, mediante oficio n.° 185-2022-CG/GRAN-OCI de 4 de mayo de 2022, registrado en el Sistema de Control Gubernamental – SCG con la orden de servicio n.° 2911-2022-009, 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 y sus modificatorias.

II. OBJETIVOS

2.1 Objetivo general

Determinar si el uso del sistema SIAF en la Municipalidad Provincial de Huarmey se realiza en cumplimiento a la normativa aplicable y disposiciones internas.

2.2 Objetivo específico

Establecer si el servidor donde se encuentra instalado el sistema SIAF se encuentra en un ambiente adecuado, si existe normativa interna que regule su uso, un sistema de gestión de seguridad de la información, así como si cuenta con un respaldo adecuado y con los mecanismos de control para el otorgamiento y administración de usuarios del SIAF, en cumplimiento a la normativa aplicable y disposiciones internas.

III. ALCANCE

El servicio de Visita de Control se desarrolló "Al uso del sistema SIAF en la Municipalidad Provincial de Huarmey", objeto del Servicio de Control que comprende establecer si el servidor donde se encuentra instalado el sistema SIAF se encuentra en un ambiente adecuado, así como si en la Entidad existe normativa interna que regule el uso del citado aplicativo, a su vez si es que se ha implementado un sistema de gestión de seguridad de la información que incluya una política y un proceso de valoración y tratamiento de riesgos, además si es que se cuenta con un plan de respaldo de la información y, finalmente, si es que existen mecanismos de control para el otorgamiento y administración de usuarios y claves de acuerdo a las responsabilidades y funciones establecidas en la normativa de los sistemas administrativos, el cual se encuentra a cargo de la Municipalidad Provincial de Huarmey, ubicada en la Plaza Independencia S/N, en el distrito de Huarmey, provincia de Huarmey, departamento de Áncash, lugar donde se desarrollan las actividades objeto de la Visita de Control, la misma que está bajo el ámbito de control del Órgano de Control Institucional responsable de la Visita de Control y que ha sido ejecutada del 4 al 10 de mayo de 2022.

IV. INFORMACIÓN RESPECTO A LA ACTIVIDAD

El servicio del control simultáneo se realizó al uso del sistema SIAF en la Municipalidad Provincial de Huarmey, objeto del Servicio de Control que comprende establecer si el servidor donde se encuentra instalado el sistema SIAF se encuentra en un ambiente adecuado, así como si en la Entidad existe normativa interna que regule el uso del citado aplicativo, a su vez si es que se ha implementado un

sistema de gestión de seguridad de la información que incluya una política y un proceso de valoración y tratamiento de riesgos, además si es que se cuenta con un plan de respaldo de la información y, finalmente, si es que existen mecanismos de control para el otorgamiento y administración de usuarios y claves de acuerdo a las responsabilidades y funciones establecidas en la normativa de los sistemas administrativos, estando orientado a comprobar el correcto y eficiente uso del sistema a través del cual, se efectúa el registro, procesamiento y generación de la información para el control del ingreso y gasto del presupuesto público, identificando las situaciones adversas que pudieran darse a lugar, con el fin de que el Titular de la entidad disponga de manera inmediata las acciones preventivas y correctivas que correspondan.

Al respecto, el SIAF, es el sistema informático de uso obligatorio por parte de las entidades del Sector Público, su objetivo es administrar y controlar los gastos e ingresos en el sector haciendo un seguimiento al presupuesto público.

Asimismo, el gasto se sujeta al proceso de ejecución presupuestal y financiera, debiendo registrarse en el SIAF los datos relacionados con su formalización en el marco de las normas legales aplicables a cada una de sus etapas: Compromiso, Devengado y Girado.

Para acceder al Sistema Integrado de Administración Financiera - SIAF, previamente a ello, los responsables del uso del sistema deberán tener instalada la última versión del SIAF desarrollada por el Ministerio de Economía y Finanzas, para luego contar con un usuario y contraseña, asignados por la Entidad, para el ingreso al sistema SIAF y sus módulos de acuerdo a sus actividades; se les otorgan los accesos, según al nivel de responsabilidad y competencia.

V. SITUACIONES ADVERSAS

De la revisión efectuada “Uso del sistema SIAF en la Municipalidad Provincial de Huarmey”, en adelante la “Entidad”, se han identificado cinco (5) situaciones adversas que afectan o podrían afectar la continuidad del proceso, el resultado o el logro de los objetivos para el inicio de la ejecución de los mismos, las cuales se exponen a continuación:

1. NO EXISTE CONTROL PARA IDENTIFICAR A LAS PERSONAS RESPONSABLES DE LOS USUARIOS SIAF, ASI COMO LOS PERMISOS CON LOS QUE CUENTAN DE ACUERDO A SUS FUNCIONES, DEBIDO A QUE EN TODAS LAS AREAS DE ADMINISTRACIÓN Y PRESUPUESTO, SE VIENE UTILIZANDO UN SOLO USUARIO “A”, SITUACIÓN QUE GENERA EL RIESGO EN LA SEGURIDAD E INTEGRIDAD DE INFORMACIÒN Y PODRÍA GENERAR ACCESOS NO AUTORIZADOS A LOS SISTEMAS DE INFORMACIÓN.

a) Condición:

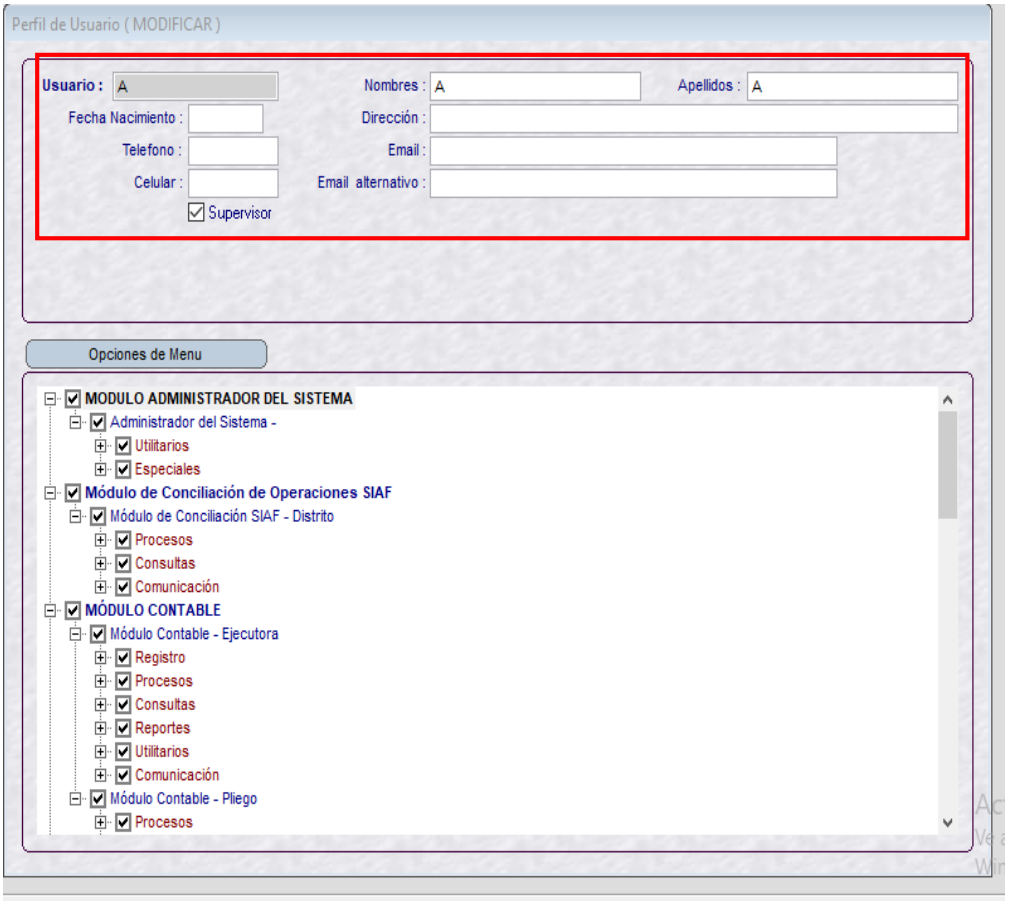
El usuario SIAF es el dispositivo que permite a los organismos públicos registrar, administrar y supervisar toda la información financiera de ingresos y gastos generados por el estado peruano; asimismo es una herramienta de uso obligatorio que todas las entidades públicas deben manejar para mantener un control de sus gastos y ajustar así sus presupuestos.

Durante la visita efectuado por la comisión de control al área de Informática, se aplicó el cuestionario Formato n.º 2 – Informática: “ Uso del Sistema Integrado de Administración Financiera – SIAF” de 4 de mayo de 2022, al Subgerente de estadística e informática[1], el cual respecto a los perfiles de los usuarios activos a la fecha no cuentan con información que permita identificar a los responsables de las cuentas , asimismo los campos correspondiente a

[1] Ing. Alejandro Castillo Salas, subgerente de estadística e informática

fecha de nacimiento, dirección, teléfono, celular, email y email alternativo , no evidencian información alguna, no permitiendo asegurar el acceso autorizado de usuario y prevenir accesos no autorizados a los sistemas de información ; debiéndose establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios; así como el registro de altas y bajas de usuarios, lo que se evidencia en la siguiente imagen:

IMAGEN Nº 1
ADMINISTRADOR DE PERFILES DE USUARIO – MODULO DE SEGURIDAD SIAF



Fuente: Formato n.º 2 informática, de 04 de mayo de 2022
Elaborado por : Comisión de Control

Así también, mediante formato n.º 3 – Administración , de 5 de mayo de 2022, el gerente de administración[2], quien respecto del manejo de los usuarios señalo lo siguiente:

"Todas las áreas administrativas de la Entidad usan el usuario "A", pero utilizan los módulos de acuerdo a sus funciones"

Seguidamente la comisión de control , se apersono a la Subgerencia de Tesorería, Contabilidad y Logística y Patrimonio , las cuales mediante consta en el Acta n.º 009-2022-CG/GRAN-OCI-MPH, de 5 de mayo de 2022, señalaron que efectivamente vienen utilizando el usuario " A", para ingresar al SIAF y realizar sus registros y operaciones; también se apersono a la Gerencia de Planeamiento y presupuesto y mediante acta n.º 010-2022-

[2] C.P.C Gustavo Nestor Chaquirre Castro

CG/GRAN-OCI-MPH, de 5 de mayo de 2022, el gerente manifestó que también viene utilizando el Usuario "A", para el ingreso al sistema.

Según lo manifestado por El sub gerente de Estadística e Informática y por la información recopilada el Usuario "A" corresponde al Administrador, pero es usado por todas las áreas de la Entidad que realizan la ejecución presupuestal con los privilegios que a continuación se detalla:

CUADRO Nº 1
LISTA DE USUARIOS SIAF Y LISTA DE PRIVILEGIOS AUTORIZADOS

Ítem	Cargo	Usuario SIAF	Módulos del SIAF asignados y privilegios autorizados	Observación
1	Gerente de Administración y Fianzas	"A"	**MODULO ADMINISTRADOR DEL SISTEMA** - Utilitarios - Especiales **MODULO DE CONCILIACIÒN DE OPERACIONES SIAF** - Proceso - Consultas - Comunicación **MODULO ADMINISTRADOR DEL SISTEMA** - Utilitarios - Especiales **MODULO CONTABLE- (Ejecutora -pliego)** **-** Registro - Proceso - Consultas - Reportes - Utilitarios - Comunicación **MODULO DEUDA PÙBLICA- Distrito** - Mantenimiento - Registro - Consultas - Reportes - Utilitarios - Comunicación **MODULO PROCESO PRESUPUESTARIO - (Entidad-Pliego)** - Registro (pliego) - Proceso - Consultas - Reportes - Utilitarios - Comunicación **MODULO DE CONTROL DE PAGO DE PLANILLAS 2014 - Ejecutora** **-** Mantenimiento - Registro - Consultas - Reportes - Utilitarios - Comunicación **MODULO ADMINISTRATIVO-Distrito** - Mantenimiento - Registro - Consultas - Reportes - Utilitarios - Comunicación	Todas las áreas que utilizan el usuario "A", tienen acceso a los módulos detallados en la columna anterior, sin restricción alguna, es así que tienen privilegios que no corresponden a sus áreas ni a sus funciones, entendiéndose de esta manera que la Entidad no tiene un adecuado control para el otorgamiento de privilegios y administración de usuarios y claves para el uso del SIAF.
2	Sub gerencia de Tesorería	"A"		
3	Sub gerencia de Contabilidad	"A"		
4	Sub gerencia de logística y patrimonio	"A"		
5	Gerencia de Planeamiento y Presupuesto	"A"		

Fuente: Información recopilada mediante: **"**Formato n.º 2- Informática, "Uso Sistema Integrado de Administración Financiera- SIAF de 04 de mayo de 2022
Elaborado por : Comisión de control

b) Criterio:

La normativa aplicable a los hechos expuestos es la siguiente:

- **Norma Técnica Peruana "/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de NTP-ISO la seguridad de la información. 2ª Edición", aprobada mediante Resolución Ministerial n.° 246-2007-PCM, publicada el 25 de agosto de 2007, que establece:**

"6.1.3 Asignación de responsabilidades sobre seguridad de la información Control.

Deberían definirse claramente las responsabilidades.

"Guía de implementación

Las asignaciones de responsabilidades sobre seguridad de la información deben hacerse en concordancia con la información de la política de seguridad (véase capítulo 4). Las responsabilidades para la protección de activos individuales y para llevar a cabo procesos de seguridad específicos deben ser claramente identificadas. (…)".

"8.1.1 Inclusión de la seguridad en las responsabilidades y funciones laborales

Control

Las funciones y responsabilidades de los empleados, (…) deben ser definidas y documentadas en concordancia con la política de seguridad de la organización".

"8.3.2 Retorno de activos
Control
Todos los empleados, (…) deben retornar todos los activos[3] de la organización que estén en su posesión hasta la finalización de su empleo, contrato o acuerdo".

"10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.1 Procedimientos y responsabilidades de operación

OBJETIVO: Asegurar la operación correcta y segura de los recursos de tratamiento de información.

Se deberían establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos de tratamiento de información. Esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.

Se implantará la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia".

"10.1.3 Segregación de tareas

Control

[3] La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada.

Se deberían segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencional, o el de un mal uso de los activos de la organización".

"11.2 Gestión de acceso de usuarios

OBJETIVO: Asegurar el acceso autorizado de usuario y prevenir accesos no autorizados a los sistemas de información.

Se debería establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios.

Estos procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios. Se debería prestar especial atención, donde sea apropiado, al necesario control de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios evitar los controles del sistema".

"11.2.1 Registro de usuarios

Control

Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario".

"11.2.2 Gestión de privilegios

Control

Debería restringirse y controlarse el uso y asignación de privilegios".

"11.2.3 Gestión de contraseñas de usuario

Control

Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal.

Guía de Implementación

El proceso debe incluir los siguientes requisitos:

a) requerir que los usuarios firmen un compromiso para mantener en secreto sus contraseñas personales (…);

b) proporcionar inicialmente una contraseña temporal segura (…) que forzosamente deben cambiar inmediatamente después;

c) establecer procedimientos para verificar la identidad de un usuario antes de proveer una contraseña nueva, de reemplazo o temporal".

"11.3 Responsabilidades de los usuarios

OBJETIVO: Evitar el acceso de usuarios no autorizados y el compromiso o hurto de la información y de las instalaciones del procesamiento de información.

Una protección eficaz necesita la cooperación de los usuarios autorizados.

Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición".

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)".

c) Consecuencia:

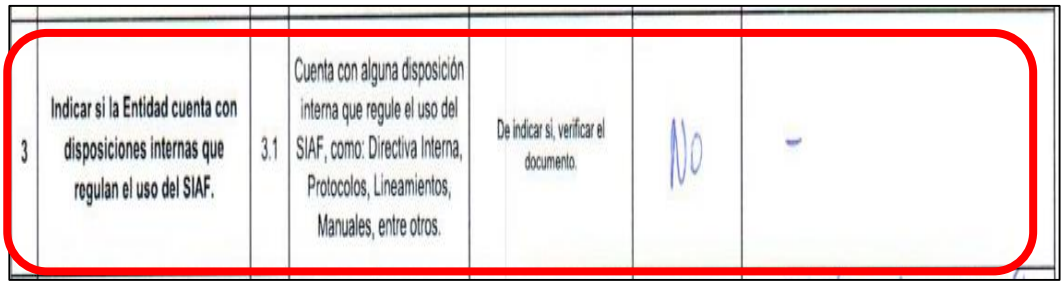
La situación antes descrita pone en riesgo la seguridad e integridad de la información y podría generar accesos no autorizados a los sistemas de información.

2. LA ENTIDAD NO CUENTA CON ALGUNA DIRECTIVA INTERNA QUE REGULE EL USO DEL SIAF, LO CUAL GENERA RIESGO DE INCUMPLIMIENTO NORMATIVO Y FALTA DE CONTROL DE LA INFORMACIÓN QUE SE ADMINISTRA MEDIANTE ESTE APLICATIVO.

a) Condición:

De la visita realizada a la oficina de Alcaldía, Sub Gerencia de Estadística e Informática y Gerencia de Administración y Finanzas, se procedió a realizar los cuestionarios contenidos en los formatos n.° 01 - "Titular de la Entidad"; formato n.° 02 - "Informática" y formato n.° 03 - "Administración", los funcionarios a cargo de cada área, manifestaron que la Entidad no cuenta con normativa interna que regule el uso del SIAF en las distintas áreas administrativas de la Entidad, a continuación se muestran los datos recopilados:

IMAGEN N° 2
EXTRACTO DE LOS FORMATOS 1, 2 Y 3



3	Indicar si la Entidad cuenta con disposiciones internas que regulan el uso del SIAF.	3.1	Cuenta con alguna disposición interna que regule el uso del SIAF, como: Directiva Interna, Protocolos, Lineamientos, Manuales, entre otros.	De indicar si, verificar el documento.	No	-

Fuente: Formatos n.°: 1, 2 y 3 – Uso del Sistema Integrado de Administración Financiera - SIAF
Elaborado por: Comisión de control.

En tal sentido, cabe resaltar que la emisión de una directiva o normativa interna que regule el uso del SIAF en la Entidad, refleja su importancia en la necesidad de regular los procedimientos que se utilizan en la administración de este aplicativo, pudiendo contener:

- La asignación de los usuarios, claves y permisos
- Procedimiento para designar a los responsables de las cuentas bancarias y su acreditación, autorizaciones para el registro de usuarios en el aplicativo.
- Procedimiento para las altas y bajas.
- El registro del perfil de usuarios y permisos.
- El cambio de contraseñas,
- Seguridad del equipo informático en donde se encuentra el servidor que almacena la información.
- La normativa aplicable a los hechos expuestos es la siguiente:

b) Criterio:

La normativa aplicable a los hechos expuestos es la siguiente:

- **Decreto Legislativo n.° 1436 Decreto Legislativo Marco de la Administración Financiera del Sector Público**, **publicado el 16 de setiembre de 2018.**
  (…)

  Artículo 2.- Principios
  Adicionalmente a los principios del Derecho Público, en lo que resulte aplicable, la Administración Financiera del Sector Público se rige por los siguientes principios:
  (…)

  2. Centralización normativa: *Consiste en la definición por parte de los entes rectores de los sistemas administrativos, de las normas de administración interna, especificando las características de cada función, su responsable y la proporción de recursos humanos asignados, para su utilización eficiente.*
  (…)
  3. Descentralización operativa: *Consiste en que las respectivas unidades dentro de las entidades del Sector Público responden a los lineamientos dados en el ámbito de la Administración Financiera del Sector Público.*
  (…)

5. Probidad: *Consiste en que los integrantes de la Administración Financiera del Sector Público adoptan las medidas o acciones pertinentes para prevenir cualquier acto de corrupción, realizando una gestión conforme a los principios y valores éticos establecidos para la función pública, garantizando su transparencia y control.*

- **Decreto Legislativo n.º 1441 - del Sistema Nacional de Tesorería, publicado el 16 de setiembre de 2018.**

CAPITULO II
ÁMBITO INSTITUCIONAL

Artículo 6.- En el nivel descentralizado u operativo
(…)
6.2. Son funciones de los responsables de la administración de los Fondos Públicos:
(…)
4. Dictar normas y procedimientos internos orientados a asegurar el adecuado apoyo económico financiero a la gestión institucional, implementando lo establecido por el ente rector.
5. Implementar y mantener las condiciones que permitan el acceso al SIAF – RP por parte de los responsables de las áreas relacionadas con la administración de la ejecución financiera y operaciones de tesorería, para el registro de la información correspondiente.

c) Consecuencia:

La situación antes descrita, podría generar el incumplimiento normativo de los usuarios del SIAF, ante la existencia de una normativa que regule su uso, así como pone en riesgo el control de la información que se administra mediante este aplicativo

3. EL AMBIENTE EN EL QUE SE ENCUENTRA ALMACENADO EL SERVIDOR SIAF DE LA ENTIDAD NO CUENTA CON MEDIDAS DE SEGURIDAD NI PROTECCIÓN, LO QUE PONDRÍA EN RIESGO LA SEGURIDAD FÍSICA DEL SERVIDOR, ASÍ COMO LA INFORMACIÓN CONTENIDA EN ÉL.

a) Condición:

Mediante formato n.° 2 “Informática”, de 5 de mayo de 2022, a través de la entrevista realizada al funcionario encargado del área en la que se encuentra almacenado el servidor SIAF, se constató que el ambiente en el que se encuentra almacenado el servidor SIAF de la Entidad no cuenta con medidas de seguridad adecuadas, puesto que no cumple con los estándares que señala la normativa vigente debido a que carece de un perímetro de seguridad definido, con barreras de seguridad y controles de entrada apropiados.

Al respecto, el funcionario responsable del área[4], en el llenado del formato en mención, señaló lo siguiente:

Pregunta 4.2.:
-El ambiente donde se encuentra ubicado el servidor que almacena la información del SIAF, cuenta con medidas y de acceso restringido.
Respuesta del funcionario

[4] Ing. Alejandro Castillo Salas, subgerente de estadística e informática.

-No.

IMAGEN N° 3
DEL EQUIPO INFORMÁTICO EN DONDE SE ENCUENTRA EL SERVIDOR QUE ALMACENA LA INFORMACIÓN DEL SIAF

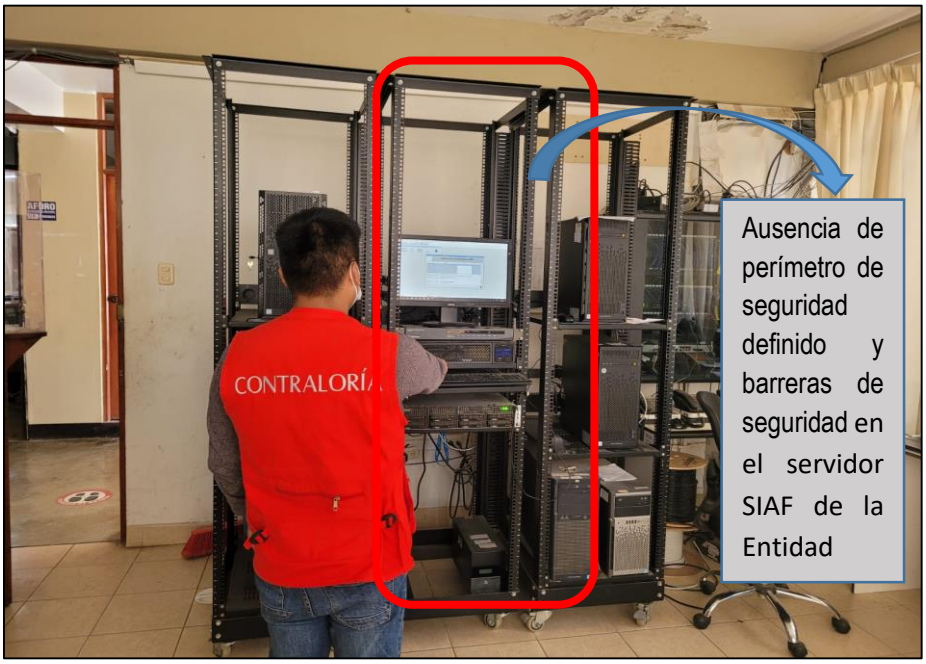
4.2	El ambiente donde se encuentra ubicado el servidor que almacena la información del SIAF, cuenta con medidas de seguridad y de acceso restringido.	SI o NO (tomar fotografias)	No
4.3	Se le ha designado formalmente la custodia del equipo informatico en el cual se encuentra el servidor que almacena la información del SIAF de la entidad.	SI o NO	No

Fuente: Formato n.° 2 - Informática, de 5 de mayo de 2022
Elaborado por: Comisión de control.

Asimismo, con el fin de dejar evidencia de la inexistencia de un ambiente adecuado para almacenar el servidor SIAF de la Entidad, se procedió a tomar muestras fotográficas en las cuales se verifica que dicho servidor no cuenta con un perímetro de seguridad definido, ni con barreras de seguridad y controles de entrada apropiados, lo cual debería de ser implementado dado que es información sensible la que se administra mediante el Sistema Integrado de Administración Financiera – SIAF.

A continuación se muestran imágenes del ambiente en el cual se encuentra el servidor SIAF de la Entidad:

IMÁGENES N° 4 y 5
AMBIENTE EN DONDE SE ENCUENTRA EL SERVIDOR SIAF DE LA ENTIDAD



Fuente: Formato n.° 2 - Informática, de 5 de mayo de 2022
Elaborado por: Comisión de control.

b) Criterio:

La normativa aplicable a los hechos expuestos es la siguiente:

- **Aprueban uso obligatorio 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. 2ª. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, aprobada mediante Resolución Ministerial n.° 246-2007-PCM publicada el 25 de agosto de 2007.**

  9. SEGURIDAD FÍSICA Y DEL ENTORNO

  9.1 Áreas seguras

  OBJETIVO: Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.

  Los recursos para el tratamiento de información crítica o sensible para la organización deberían ubicarse en áreas seguras protegidas por un perímetro de seguridad definido, con barreras de seguridad y controles de entrada apropiados. Se debería dar protección física contra accesos no autorizados, daños e interferencias.
  Dicha protección debería ser proporcional a los riesgos identificados"

  9.1.1 Perímetro de seguridad física

  Control

Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información e recursos de procesamiento de información".

9.1.2 Controles físicos de entradas Control

Control

Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso sólo al personal autorizado".

"9.2.1 Instalación y protección de equipos

Control

El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados".
(…)

c) Consecuencia:

La situación antes descrita pone en riesgo la seguridad física del servidor SIAF de la Entidad, así como la información contenida en él.

4. LA ENTIDAD NO HA IMPLEMENTADO UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN QUE INCLUYA UNA POLÍTICA Y UN PROCESO DE VALORACIÓN Y TRATAMIENTO DE RIESGOS; LO CUAL PODRÍA AFECTAR LA PRESERVACIÓN DE LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN REGISTRADA EN EL SIAF.

a) Condición:

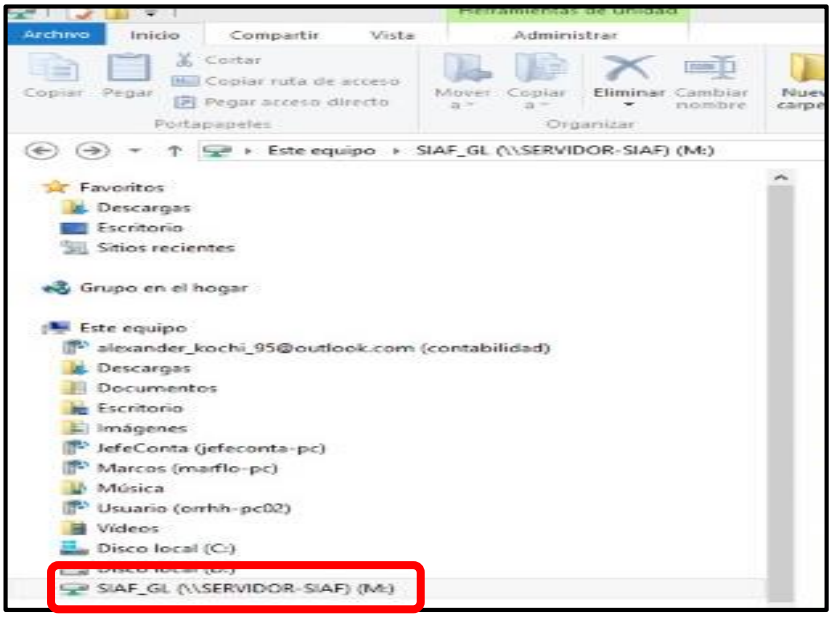
De acuerdo con la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", es obligación de la Entidad implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información para sus sistemas informáticos; asimismo, la alta dirección debe establecer una política de seguridad de la información.

Además, se debe definir y aplicar un proceso de valoración del riesgo de seguridad de la información para identificar riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información y determinar todos los controles que son necesarios en sus sistemas informáticos, entre ellos, el Sistema Integrado de Administración Financiera – SIAF.

Al respecto, durante la visita realizada por la comisión de control el día 04 de mayo de 2021, Mediante el Formato n.° 2 – Informática- "Uso del Sistema Integrado de administración Financiera SIAF. Se verificó que la Entidad no ha implementado una política de seguridad informática o *controles de seguridad que restrinja permisos como instalación de softwares, bloqueos de páginas, bloqueos de puertos USB, en los usuarios de equipos informáticos que se asignan a los trabajadores*.

Además el Subgerente de Estadística e Informática, *señalo que todos los usuarios se conectan mediante la carpeta compartida SIAF, lo que es una forma insegura, puesto que al tener acceso a la carpeta compartida, pueden escribir, eliminar archivos, incluso hacer una copia de la data sin autorización debida.*

IMAGEN Nº 6
CARPETA COMPARTIDA DEL SIAF



Fuente: servidor SIAF

b) Criterio.

La normativa aplicable a los hechos expuestos es la siguiente:

- **Resolución Ministerial n.° 004-2016-PCM publicada en el diario oficial "El Peruano" el 14 de enero de 2016, modificada mediante Resolución Ministerial n.° 166-2017-PCM de 20 de junio de 2017, que 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 de la Información. Requisitos. 2a Edición", en todas las entidades integrantes del Sistema Nacional de Informática.**

  4. CONTEXTO DE LA ORGANIZACIÓN
  (…)
  4.4 Sistema de gestión de seguridad de la información La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, en conformidad con los requisitos de esta Norma Técnica Peruana.
  (…)

  5. LIDERAZGO
  (…)
  5.2 Política

La alta dirección debe establecer una política de seguridad de la información que:

(…)

6. PLANIFICACIÓN

6.1. Acciones para tratar los riesgos y las oportunidades

(…)

6.1.2. Valoración del riesgo de seguridad de la información
La organización debe definir y aplicar un proceso de valoración del riesgo de seguridad de la información que:
(…)

6.1.3 Tratamiento de riesgos de seguridad de la información
La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para:

c) Consecuencia:

La situación expuesta podría afectar la preservación de la confidencialidad, integridad disponibilidad de la información relacionada a las operaciones realizadas en el SIAF.

5. LA ENTIDAD NO HA DEFINIDO UN PLAN DE RESPALDO DE LA INFORMACIÓN, NO CUENTA CON UN DIRECTORIO EN UN MEDIO DE ALMACENAMIENTO INDEPENDIENTE PARA LA INFORMACIÓN RESPALDADA; LO CUAL PODRÍA AFECTAR LA PROTECCIÓN, INTEGRIDAD Y SEGURIDAD DE LA INFORMACIÓN REGISTRADA EN EL SIAF, ANTE LA OCURRENCIA DE CUALQUIER CONTINGENCIA EN EL SERVIDOR.

a) Condición:

De acuerdo con la Resolución Jefatural n.º 386-2002-INEI del 31 de diciembre de 2002, que aprueba la Directiva "Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Pública", la Entidad debe tomar las medidas necesarias para proteger y salvaguardar la integridad y seguridad de la información.

Además, debe establecer un programa de revisión de la información respaldada en medios de almacenamiento independiente, de acuerdo con la importancia que ésta tenga para la Entidad, el cual será establecido por el responsable de la función de respaldo de la información de los sistemas informáticos, entre ellos, el Sistema Integrado de Administración Financiera (SIAF).

Al respecto, durante la visita realizada el 04 de mayo de 2022, mediante la aplicación del formato n.º 2 – Informática – "Uso del Sistema Integrado de Administración Financiera –SIAF" , *El subgerente de Estadística e Informática, manifestó que si se realiza el respaldo de la información diariamente, en el mismo esquipo del servidor, sin embargo, se verificó que la Entidad no tiene definido un plan de respaldo de la información, no cuenta con un "Directorio" en un medio de almacenamiento independiente que permita salvaguardar la información respaldada; asimismo, no informa periódicamente a los usuarios el cronograma de respaldo.* *(Subrayado agregado)*

Así también, El Gerente de Administración y Finanzas, mediante la aplicación del formato n.º 3 – Administración – "Uso del Sistema Integrado de Administración Financiera –SIAF", de 05 de mayo de 2022, señalo que no se realiza respaldo de la información del SIAF, a través de back ups en la Entidad.

b) Criterio:

La situación expuesta no es concordante con la normativa señalada a continuación:

- **Resolución Jefatural n.° 386-2002-INEI de 31 de diciembre de 2002, que aprueba Directiva "Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las entidades de la Administración Pública"**

"(…)

V. DISPOSICIONES GENERALES

(…)

5.1 Toda información guardada contará con un Directorio en un medio de almacenamiento independiente que permita conocer todas las características y facilite la plena identificación de la información respaldada.

5.2. Las Oficinas de Informática (o la que haga sus veces) de las entidades de la administración pública, deberán definir un plan de respaldo de la información, de acuerdo a factores legales, institucionales y otros.

(…)

VI. DISPOSICIONES ESPECÍFICAS

6.4 DEL RESPALDO

(…)

6.4.9 La Oficina de Informática (o la que haga sus veces) informará periódicamente a los usuarios, el cronograma de respaldo de información, asimismo, hará de conocimiento general las políticas de seguridad y respaldo de información.

(…)"

c) Consecuencia:

La situación expuesta podría afectar la protección, integridad y seguridad de la información registrada SIAF, puesto que no existe un medio independiente externo de almacenamiento para su respaldo.

VI. DOCUMENTACIÓN VINCULADA A LA ACTIVIDAD

La información y documentación que la comisión de control ha revisado y analizado durante el desarrollo del servicio de visita de control "Uso del Sistema SIAF en la Municipalidad Provincial de Huarmey", se encuentra detallada en el **Apéndice n.° 1**.

Las situaciones adversas identificadas en el presente informe se sustentan en la revisión y análisis de la documentación e información obtenida por la comisión de control, la cual ha sido señalada en la condición y se encuentra en el acervo documentario de la Entidad.

VII. INFORMACIÓN DEL REPORTE DE AVANCE ANTE SITUACIONES ADVERSAS

Durante la ejecución del presente servicio de visita de control, la comisión de control no emitió el reporte de avance ante situaciones adversas.

VIII. CONCLUSIÓN

Durante la ejecución del servicio de visita de control al uso del sistema SIAF en la Municipalidad Provincial de Huarmey, se han advertido cinco (5) situaciones adversas que afectan o podrían afectar la continuidad del proceso, el resultado o el logro de los objetivos del uso del sistema SIAF, las cuales han sido detalladas en el presente informe.

IX. RECOMENDACIONES

1. Hacer de conocimiento al Titular de la Entidad el presente informe de visita de control, el cual contiene las situaciones adversas identificadas como resultado del servicio de visita de control al uso del sistema SIAF, con la finalidad que 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 de la visita de control.

2. Hacer de conocimiento al Titular de la Entidad que debe comunicar al Órgano de Control Institucional, a través del plan de acción, las acciones preventivas o correctivas que implemente respecto a las situaciones adversas contenidas en el presente informe de visita de control.

Huarmey, 16 de mayo de 2022.

Ing.Carlos José Peje Quesada
Supervisor
Comisión de Control

C.P.C. Persyval Vásquez Núñez
Jefe de Comisión
Comisión de Control

Ing. Carlos José Peje Quesada
Jefe del Órgano de Control Institucional
Municipalidad Provincial de Huarmey

APÉNDICE N° 1

DOCUMENTACIÓN VINCULADA A LA ACTIVIDAD

NO EXISTE CONTROL PARA IDENTIFICAR A LAS PERSONAS RESPONSABLES DE LOS USUARIOS SIAF, ASI COMO LOS PERMISOS CON LOS QUE CUENTAN DE ACUERDO A SUS FUNCIONES, DEBIDO A QUE EN TODAS LAS AREAS DE ADMINISTRACIÓN Y PRESUPUESTO, SE VIENE UTILIZANDO UN SOLO USUARIO "A", SITUACIÓN QUE GENERA EL RIESGO EN LA SEGURIDAD E INTEGRIDAD DE INFORMACIÒN Y PODRÍA GENERAR ACCESOS NO AUTORIZADOS A LOS SISTEMAS DE INFORMACIÓN.

Nº	Documento
1	Formato n.° 2 - Informática, de 5 de mayo de 2022
2	Acta n.º 009 y 10 -2022-CG/GRAN-OCI-MPH, de 5 de mayo de 2022
3	Formato n.° 3 – Administración, de 5 de mayo de 2022

LA ENTIDAD NO CUENTA CON ALGUNA DIRECTIVA INTERNA QUE REGULE EL USO DEL SIAF, LO CUAL GENERA RIESGO DE INCUMPLIMIENTO NORMATIVO Y FALTA DE CONTROL DE LA INFORMACIÓN QUE SE ADMINISTRA MEDIANTE ESTE APLICATIVO.

Nº	Documento
1	Formato n.° 1 - Titular de la Entidad, de 9 de mayo de 2022
2	Formato n.° 2 - Informática, de 5 de mayo de 2022
3	Formato n.° 3 – Administración, de 5 de mayo de 2022

EL AMBIENTE EN EL QUE SE ENCUENTRA ALMACENADO EL SERVIDOR SIAF DE LA ENTIDAD NO CUENTA CON MEDIDAS DE SEGURIDAD NI PROTECCIÓN, LO QUE PONDRÍA EN RIESGO LA SEGURIDAD FÍSICA DEL SERVIDOR, ASÍ COMO LA INFORMACIÓN CONTENIDA EN ÉL.

Nº	Documento
1	Formato n.° 2 - Informática, de 5 de mayo de 2022

LA ENTIDAD NO HA IMPLEMENTADO UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN QUE INCLUYA UNA POLÍTICA Y UN PROCESO DE VALORACIÓN Y TRATAMIENTO DE RIESGOS; LO CUAL PODRÍA AFECTAR LA PRESERVACIÓN DE LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN REGISTRADA EN EL SIAF.

Nº	Documento
1	Formato n.° 2 - Informática, de 5 de mayo de 2022

LA ENTIDAD NO HA DEFINIDO UN PLAN DE RESPALDO DE LA INFORMACIÓN, NO CUENTA CON UN DIRECTORIO EN UN MEDIO DE ALMACENAMIENTO INDEPENDIENTE PARA LA INFORMACIÓN RESPALDADA; LO CUAL PODRÍA AFECTAR LA PROTECCIÓN, INTEGRIDAD Y SEGURIDAD DE LA INFORMACIÓN REGISTRADA EN EL SIAF, ANTE LA OCURRENCIA DE CUALQUIER CONTINGENCIA EN EL SERVIDOR

Nº	Documento
2	Formato n.° 2 - Informática, de 5 de mayo de 2022
3	Formato n.° 3 – Administración, de 5 de mayo de 2022

LA CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

"Año del Fortalecimiento de la Soberanía Nacional"
"Decenio de la igualdad de oportunidades para mujeres y hombres"

Huarmey, 16 de mayo de 2022.

MUNICIPALIDAD PROVINCIAL DE HUARMEY
TRAMITE DOCUMENTARIO
RECIBIDO
17 MAYO 2022
Código: 20220 7658 Hora: 3:05P
Folio: 19 Firma:
La recepción de este documento no implica la conformidad del mismo

OFICIO N° 192-2022-CG/GRAN-OCI-MPH
Señor:
Elmer Dueñas Espíritu
Alcalde
Municipalidad Provincial de Huarmey
Plaza Independencia S/N
Huarmey/Huarmey/Áncash

ASUNTO : Remisión de informe de visita de control N° 008-2022-OCI/2911-SVC.

REF. : 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, el Órgano de Control Institucional de la Municipalidad Provincial de Huarmey dispuso la realización del servicio de control simultáneo – Visita de Control a la: "**Uso del sistema SIAF en la Municipalidad Provincial de Huarmey",** en la Municipalidad Provincial de Huarmey, distrito de Huarmey, provincia de Huarmey, departamento de Áncash". En tal sentido, comunicamos que se han identificado cinco (5) situaciones adversas contenidas en el Informe de Visita de Control N° 008-2022-OCI/2911-SVC, que se adjunta al presente documento.

En tal sentido, solicitamos remitir al Órgano de Control Institucional, el Plan de Acción correspondiente, en un plazo de diez (10) días hábiles contados a partir del día siguiente hábil de recibida la presente comunicación.

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

Atentamente,

LA CONTRALORÍA
Firmado digitalmente por PEJE QUESADA Carlos Jose FAU 20131378972 soft
Motivo: Soy el autor del documento
Fecha: 16-05-2022 12:26:52 -05:00

Documento firmado digitalmente
Ing. Carlos José Peje Quesada
Jefe del Órgano de Control Institucional
Municipalidad Provincial de Huarmey

V°B°
Firmado digitalmente por PEJE QUESADA Carlos Jose FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 16-05-2022 12:27:25 -05:00

Se adjunta informe n.° 008-2022-OCI/2911-SVC
En (19) folios
C/c
Archivo
P/T
CPQ/epb