Resolución Directoral

RESOLUCIÓN DIRECTORAL N° 00004-2025-VIVIENDA/OGEI

San Isidro, 09 de Mayo de 2025

VISTOS:

El informe N° 41-2025/OGEI-GFERNANDEZ del Oficial de Seguridad de la Información; y,

CONSIDERANDO:

Que, mediante Decreto Supremo N° 004-2013-PCM, se aprueba la Política Nacional de Modernización de la Gestión Pública, siendo el principal instrumento orientador de la modernización de la gestión pública en el Perú, que establecerá la visión, los principales lineamientos para una actuación coherente y eficaz del sector público, al servicio de lo ciudadanos y el desarrollo del país; agregando en el numeral 3.2 los ejes transversales de la Política de Modernización en el Gobierno Electrónico;

Que, el artículo 55 del Reglamento de Organización y Funciones - ROF del Ministerio de Vivienda, Construcción y Saneamiento MVCS, establece que la Oficina General de Estadística e Informática - OGEI, es el órgano encargado responsable de la gestión de la infraestructura de tecnologías de la información y comunicaciones, así como planificar, desarrollar, implementar y gestionar proyectos de desarrollo de soluciones basadas en tecnologías de la información y comunicación para la administración y gestión de la informática estadística sectorial;

Que, con Resolución Directoral N° 022-2022-INACAL/DN, se aprueba la NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3a Edición, el cual reemplaza a la NTP-ISO/IEC 27001:2014;

Que, la referida Norma Técnica Peruana NTP-ISO/IEC 27001 señala en el Anexo control A.8.7 de la ISO/IEC 27001:2022,. Control. La protección contra programas maliciosos (malware) debe implementarse y respaldar la toma de conciencia adecuada del usuario.

Que, con Resolución Ministerial No 356-2018-VIVIENDA, del 23 de octubre de 2018 se constituyó el Comité de Gobierno Digital en el marco de la Resolución Ministerial N° 119-2018-PCM, entre cuyas funciones destaca la de liderar y dirigir el proceso de transformación digital en la entidad;

Que, mediante el informe N° 41-2025/OGEI-GFERNANDEZ, el Oficial de Seguridad de la Información comunica que respecto a las materias de su competencia se ha emitido opinión favorable respecto a la aprobación de las citadas disposiciones;

Que, estando a lo expuesto y conforme a la propuesta remitida por el Oficial de Seguridad de la Información, contando con la opinión favorable de la Oficina de Tecnologías de la Información, corresponde expedir la presente Resolución aprobando las “Disposiciones que regulan el uso del escritorio y pantalla limpia en el MVCS”, según lo expresado en los documentos de visto;

SE RESUELVE:

Artículo 1.- Aprobar las “Disposiciones de protección contra programas maliciosos”, el mismo que forma parte integrante de la presente Resolución.

Artículo 2.- Disponer la publicación de la presente Resolución en el Portal Institucional del Ministerio de Vivienda, Construcción y Saneamiento.

Regístrese y comuníquese.

FIRMA DIGITAL
PERÚ Ministerio de Vivienda, Construcción y Saneamiento
VIVIENDA
Firmado digitalmente por: CAMACHO ZARATE Daniel Alfonso FAU 20504743307 hard
Motivo: Soy el autor del documento
Fecha: 2025/05/09 18:38:27-0500

Firmado digitalmente por
DANIEL ALFONSO CAMACHO ZARATE
DIRECTOR GENERAL
OFICINA GENERAL DE ESTADISTICA E INFORMATICA
Ministerio de Vivienda, Construcción y Saneamiento

DISPOSICIONES DE PROTECCIÓN CONTRA PROGRAMAS MALICIOSOS

Nombre	Cargo	Visto
Elaborado por: Guillermo Pedro Fernández Namuche	Especialista en Seguridad de la Información	FIRMA DIGITAL VIVIENDA Firmado digitalmente por:FERNÁNDEZ NAMUCHE Guillermo Pedro FAU 20504743307 soft Motivo: En señal de conformidad Fecha: 2025/05/08 11:37:54-0500
Revisado por: Johnny Albino Tarmeño Chavarria	Director de la OTI	FIRMA DIGITAL VIVIENDA Firmado digitalmente por:TARMEÑO CHAVARRIA Johnny Albino FAU 20504743307 hard Motivo: En señal de conformidad Fecha: 2025/05/08 14:10:45-0500
Kenny Mirko Rodriguez Cáceres	Coordinador de Infraestructura Tecnológica	FIRMA DIGITAL VIVIENDA Firmado digitalmente por:RODRIGUEZ CACERES Kenny Mirko FAU 20504743307 soft Motivo: En señal de conformidad Fecha: 2025/05/08 11:56:58-0500
Felix Rodolfo Rodriguez Paredes	Asistente de Soporte Técnico	FIRMA DIGITAL VIVIENDA Firmado digitalmente por:RODRIGUEZ PAREDES Felix Rodolfo FAU 20504743307 soft Motivo: Soy el autor del documento Fecha: 2025/05/08 12:26:51-0500
Aprobado por: Daniel Alfonso Camacho Zarate	Director General de la OGEI	FIRMA DIGITAL VIVIENDA Firmado digitalmente por:CAMACHO ZARATE Daniel Alfonso FAU 20504743307 hard Motivo: En señal de conformidad Fecha: 2025/05/08 15:22:15-0500

Registro de Cambios			
Versión	**Páginas**	**Fecha**	**Descripción**
1.0	8	08.05.2025	Versión inicial

I. OBJETIVO

Asegurar la protección robusta de la información ante la amenaza persistente de programas con código malicioso, tales como spyware y malware, en concordancia con la NTP-ISO/IEC 27001.

II. ALCANCE

Las disposiciones del presente documento son de obligatorio cumplimiento para todas las partes interesadas, instalaciones y activos de información (incluyendo equipos de comunicación e infraestructura de red) que participan en la provisión de los servicios ofrecidos por el MVCS.

III. BASE NORMATIVA

3.1 Ley N° 30096 y su modificatoria Ley 30171: Ley de Delitos Informáticos.
3.2 Ley N° 29733: Ley de Protección de Datos Personales y su reglamento.
3.3 Decreto Supremo N° 010-2014-VIVIENDA, establece las funciones de la Oficina de Tecnología de la Información.
3.4 Decreto Legislativo N°1412, que aprueba la Ley de Gobierno Digital.
3.5 Resolución Legislativa N° 30913, Resolución Legislativa que aprueba el convenio sobre La ciberdelincuencia.
3.6 Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la Resolución Ministerial N° 004-2016-PCM.
3.7 NTP-ISO/IEC 27001:2022 - control A.8.7 (Protección contra programas maliciosos - malware).

IV. DEFINICIONES

4.1 **Control:** Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

4.2 **Incidente de Seguridad:** Evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad por una amenaza que intenta quebrar los mecanismos de seguridad existentes.

4.3 **Malware:** Llamado también software malicioso o software malintencionado, diseñado para llevar a cabo acciones no deseadas y sin el consentimiento explícito del usuario.

4.4 **Medio removible:** Dispositivo de almacenamiento de información lógica en el que se pueden grabar, remover o modificar dicha información, con la finalidad de transportarla fácilmente. Ejemplo: memorias USB, discos compactos, tarjetas SD, cintas de respaldo, entre otros.

4.5 **Ransomware:** Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que, si la víctima no paga el rescate, no podrá acceder a ella.

4.6 **Riesgo:** Probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en el Ministerio.

4.7 **Spyware:** Programa espía es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

4.8 **Usuario:** Persona que labora o presta servicios independientemente del régimen laboral o modalidad contractual y que utiliza el servicio de internet institucional para llevar a cabo diversas actividades relacionadas con sus funciones.

4.9 **Virus informático:** Malware que tiene como característica principal que infecta ficheros ejecutables o sectores de arranque de dispositivos de almacenamiento.

4.10 **Vulnerabilidad:** Debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

V. ABREVIATURAS

5.1 **MVCS:** Ministerio de Vivienda, Construcción y Saneamiento
5.2 **NTP:** Norma Técnica Peruana
5.3 **OTI:** Oficina de Tecnología de la Información
5.4 **OGEI:** Oficina General de Estadística e Informática
5.5 **SGSI:** Sistema de Gestión de Seguridad de la Información
5.6 **VPN:** Red Privada Virtual

VI. SOBRE LA PROTECCIÓN CONTRA PROGRAMAS MALICIOSOS

6.1 La OGEI a través de la OTI, será responsable de instalar, configurar, monitorear y controlar la plataforma de antivirus tanto a nivel de servidores

como a nivel de los equipos de usuario final (equipos de computo, equipos portátiles, entre otros) asignados por el Ministerio en las distintas sedes.

6.2 Para la conexión de equipos de cómputo que no sean propiedad del MVCS a la red institucional, el área usuaria deberá formalizar una solicitud a la Mesa de Servicios a través de los canales oficiales. Dicha solicitud debe contar con la autorización del Director/a o Jefe inmediato del área correspondiente. Además, el equipo será sometido a una revisión técnica por parte del equipo de soporte, y deberá cumplir con los siguientes requisitos:

a) El equipo debe contar con un software antivirus que tenga una licencia válida durante todo el periodo de la relación contractual con el MVCS. Previamente, se deberá realizar una actualización de la base de firmas del antivirus y efectuar un escaneo exhaustivo de todas las unidades locales del equipo. Los resultados del escaneo no deben mostrar la presencia de software malicioso. Si se detecta software malicioso, el equipo no podrá conectarse a la red interna hasta que se complete su desinfección.
b) La OTI implementará restricciones para bloquear la descarga de archivos ejecutables durante la navegación por Internet, con el fin de proteger la red institucional.
c) Todo software que no cuente con la correspondiente licencia deberá ser desinstalado de inmediato. La falta de soporte oficial del fabricante convierte estos programas en una potencial vulnerabilidad que podría comprometer la seguridad de la red interna del MVCS.
d) Los equipos que no cumplan con los requisitos mencionados anteriormente no podrán establecer conexión a la red interna hasta que las deficiencias sean debidamente corregidas.
e) Los equipos autorizados deberán permanecer en las instalaciones del MVCS durante la vigencia del contrato para evitar riesgos asociados a la conexión a redes externas comprometidas.

6.3 El usuario deberá informar de inmediato a la Mesa de Servicios a través de los canales oficiales en caso de detectar alguno de los siguientes incidentes relacionados con la seguridad del equipo de cómputo o laptop:

a) El equipo no cuenta con un software antivirus instalado.
b) La base de datos de firmas del antivirus presenta fallos en la actualización (desactualizado), lo que podría comprometer la protección contra amenazas conocidas.

c) El software antivirus institucional no se encuentra ejecutándose.
d) El antivirus ha detectado virus en los archivos del equipo.
e) Aparición de ventanas emergentes en el escritorio en idioma español o inglés solicitando rescate, lo que puede indicar la presencia de un ataque de ransomware.
f) Los nombres de los archivos o carpetas empiezan a cambiar de forma irregular, utilizando símbolos especiales y/o caracteres alfanuméricos.
g) Los archivos empiezan a ocultarse, cambiar de extensión o eliminarse automáticamente sin intervención del usuario.
h) Aparición de una gran cantidad de correos "Sin Asunto" o sin remitente en la bandeja de entrada del correo electrónico institucional, lo que puede ser indicativo de un ataque de phishing o propagación de malware.

El equipo de infraestructura de la OTI será responsable de supervisar la consola del antivirus institucional para identificar los equipos con problemas relacionados con el software antivirus y/o la actualización de las firmas. Esta supervisión se llevará a cabo conforme al **"Procedimiento de control de atención de PC's con problemas de antivirus[1]"**, asegurando que cualquier incidente sea identificado y mitigado rápidamente para proteger la red institucional y la seguridad de la información.

6.4 La OTI debe implementar controles que prevengan o detecten el uso de software no autorizado en la infraestructura del MVCS, mediante la implementación de una lista blanca de aplicaciones, asegurando que solo las aplicaciones previamente aprobadas y verificadas puedan ejecutarse en los equipos de cómputo y servidores.

6.5 La OTI a través de la Mesa de Servicios es responsable de la instalación y actualización del software antivirus en todos los equipos de cómputo y el equipo de infraestructura en los servidores del MVCS, antes de ser conectado a la red institucional.

6.6 La OTI debe implementar los mecanismos de seguridad para garantizar que ningún usuario u otra persona tenga el privilegio de suspender o deshabilitar la protección del antivirus, a menos que cuente con la autorización expresa de la OTI.

6.7 La OGEI no envía correos electrónicos con vínculos directos solicitando información confidencial. En caso de recibir un correo de este tipo, el

[1] https://www.gob.pe/institucion/vivienda/normas-legales/4823962-007-2023-vivienda-ogei

destinatario debe comunicarse con el área que solicitó la información para verificar la autenticidad del mensaje, asegurando la protección de la información sensible.

6.8 La OTI debe mantener actualizado el sistema operativo de todos los equipos de cómputo y servidores del MVCS. Los sistemas operativos deben recibir actualizaciones de seguridad periódicas para minimizar las vulnerabilidades que puedan ser explotadas por atacantes.

6.9 La OTI debe realizar análisis programados de seguridad en las unidades locales de los equipos de cómputo y servidores del MVCS. Esto incluye la ejecución de escaneos antivirus periódicos para identificar y mitigar posibles riesgos de seguridad.

6.10 Se insta al usuario a ejercer precaución al acceder a los sistemas en línea o al correo institucional desde equipos de dudosa confiabilidad o mediante redes Wi-Fi públicas no seguras. En su lugar, se recomienda utilizar la red de datos móviles o emplear la VPN o los servicios proporcionados por el MVCS, garantizando la seguridad de las comunicaciones.

6.11 El usuario debe abstenerse de utilizar medios extraíbles (USB) que hayan sido previamente conectados a equipos externos al MVCS. En caso de requerir su uso, se procederá al análisis y desinfección del dispositivo mediante el antivirus institucional al ser insertado en el equipo correspondiente, asegurando que no se introduzcan amenazas a la red institucional.

VII. EL USUARIO ESTÁ PROHIBIDO DE:

7.1 Manipular o ejecutar software desde dispositivos de almacenamiento que se consideren sospechosos por contener software malicioso, o cuya fuente de emisión no sea verificable. En caso de requerir la instalación de algún software, se deberá solicitar a la OTI a través de la Mesa de Servicios. La instalación de dicho software estará sujeta a evaluación, aprobación y ejecución exclusiva por parte de la OTI.

7.2 Instalar, desinstalar o copiar cualquier tipo de software en cualquier equipo de cómputo o servidor perteneciente al Ministerio sin la debida autorización de la OTI.

7.3 Insertar cualquier dispositivo de almacenamiento encontrado en las dependencias del MVCS sin una revisión previa. Cualquier incidente

relacionado con este tipo de dispositivos deberá ser notificado de inmediato a la Mesa de Servicios mediante los canales oficiales, para que se realice el análisis pertinente del contenido del dispositivo y se determine si representa un riesgo para la seguridad de la red institucional.

7.4 Abrir archivos adjuntos no solicitados, incluso si aparentan provenir de una fuente confiable. En caso de sospecha de que el equipo de cómputo está infectado con virus, el incidente debe ser reportado de inmediato a la OTI a través de la Mesa de Servicios, utilizando los canales oficiales para su pronta atención y mitigación del riesgo.

7.5 Acceder a sitios web de videojuegos, publicidad, ofertas, contenido sexual o enlaces de carácter personal, así como la descarga de archivos ejecutables desde cualquier repositorio de Internet.

7.6 Queda estrictamente prohibido conectar equipos personales a la red interna sin la debida autorización y coordinación con la OTI. La seguridad física de los equipos es responsabilidad del área usuaria.

VIII. RECOMENDACIONES

Responsabilidades del usuario en la conexión a la red informática del Ministerio con equipos informáticos personales y/o que realicen teletrabajo parcial o total:

8.1 Proteger la información, a la que tiene acceso, de amenazas como accesos no autorizados, alteración indebida o software malicioso, cumpliendo con lo siguiente:

a) Conectarse exclusivamente desde ambientes físicos que ofrezcan seguridad comprobada.
b) Establecer conexiones únicamente a través de accesos a internet de confianza, evitando el uso de redes públicas o gratuitas.
c) Asegurar la protección de las redes domésticas mediante la implementación de contraseñas de acceso robustas para la red inalámbrica (WiFi).
d) Otorgar acceso al equipo informático al personal autorizado de Mesa de Servicios de la OTI para la verificación de la actualización del sistema operativo y antivirus, así como para la confirmación de que las aplicaciones cuenten con las últimas actualizaciones disponibles.
e) Activar el bloqueo de pantalla del equipo de computo en momentos de inactividad o ausencia del puesto de trabajo.
f) Ubicarse en un espacio que asegure la privacidad del trabajo,

evitando la visibilidad a terceros.

8.2 El usuario debe garantizar que el equipo informático conectado a través de la VPN del Ministerio no se conecte simultáneamente a ninguna otra red, salvo aquella red personal que esté bajo su control directo y que cumpla con las medidas mínimas de seguridad.

8.3 Se deben adoptar las medidas necesarias para garantizar que el entorno físico de trabajo disponga de acceso a la red alámbrica o inalámbrica (WIFI) estable, libre de interrupciones que puedan afectar la continuidad operativa o el desempeño laboral. Esto implica asegurar una conexión a internet de alta disponibilidad y confiabilidad.

8.4 Toda actividad realizada bajo la modalidad de teletrabajo debe ser resguardada exclusivamente en la plataforma institucional Google Workspace, a fin de asegurar la confidencialidad, integridad y disponibilidad de la información institucional. El único repositorio autorizado para el almacenamiento de documentos de trabajo es "Mi unidad" de Google Drive, conforme a las disposiciones establecidas por la OTI, lo cual permite implementar medidas efectivas de control de acceso, respaldo y prevención de pérdida de datos.

IX. REVISIÓN Y ACTUALIZACIÓN

En concordancia con lo dispuesto en la norma ISO/IEC 27001:2022, el Oficial de Seguridad de la Información, en coordinación con la OGEI a través de la OTI, realizará anualmente una revisión integral de las disposiciones vigentes en materia de seguridad de la información. Esta revisión tiene como finalidad evaluar su efectividad, identificar oportunidades de mejora y actualizar las directrices conforme a los avances tecnológicos, cambios normativos y lecciones aprendidas, como parte del proceso de mejora continua del SGSI.