DIRECTIVA GENERAL N° 006-2024-VIVIENDA-DM
DISPOSICIONES QUE REGULAN EL USO DEL CORREO ELECTRÓNICO EN EL MINISTERIO DE VIVIENDA, CONSTRUCCIÓN Y SANEAMIENTO

Formulada por: Oficina General de Estadística e Informática

I. OBJETIVO

Establecer disposiciones que regulen la gestión, monitoreo, control, seguridad y privacidad de los servicios del correo electrónico en el Ministerio de Vivienda, Construcción y Saneamiento, (en adelante MVCS), Programa Nacional de Saneamiento Rural, Programa Nacional de Saneamiento Urbano y Programa Agua Segura para Lima y Callao, (en adelante Programas), así como, precisar los riesgos y establecer las pautas en el uso de estos servicios por los usuarios.

II. FINALIDAD

2.1 Garantizar el uso adecuado de los servicios contratados de correo electrónico en el MVCS.

2.2 Contribuir en la productividad, disponibilidad, integridad, privacidad y la seguridad de la información a nivel institucional.

III. ALCANCE

La presente Directiva es de alcance y aplicación obligatoria para todos los Órganos, Unidades Orgánicas, Programas (PNSR, PNSU y PASLC) y otras dependencias del Ministerio de Vivienda, Construcción y Saneamiento.

IV. BASE LEGAL

4.1 Ley N° 30096, Ley de delitos informáticos y modificatorias
4.2 Ley N° 27815, Ley del Código de Ética de la Función Pública y modificatorias.
4.3 Ley N° 29733, Ley de Protección de Datos Personales y modificatorias.
4.4 Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) y modificatorias.
4.5 Ley N° 30225, Ley de Contrataciones del Estado y su reglamento.
4.6 Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales aprobado por Decreto Supremo 003-2013-JUS.
4.7 Decreto Supremo N° 072-2003-PCM que aprueba el Reglamento de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública y modificatorias.
4.8 Decreto Supremo N° 010-2014-VIVIENDA, que aprueba el Reglamento de Organización y Funciones del Ministerio de Vivienda, Construcción y Saneamiento - ROF.
4.9 Decreto Supremo N° 006-2015-VIVIENDA, que modifica el ROF.
4.10 Decreto Supremo N° 021-2019-JUS que aprueba el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública aprobado por el Decreto Supremo N° 021-2019-JUS.
4.11 Reglamento de Organización y Funciones del Ministerio de Vivienda, Construcción y Saneamiento, aprobado por Decreto Supremo N° 010-2014-VIVIENDA y modificatorias
4.12 Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 27001:2014 EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da. Edición” (en adelante NTP-ISO/IEC 27001:2014), en todas las entidades integrantes del Sistema Nacional de Informática.

4.13 Resolución Ministerial N° 072-2016-VIVIENDA, se crea el Comité de Gestión de Seguridad de la Información, conformado, entre otros, por el/la Oficial de Seguridad de la Información.

4.14 Resolución Ministerial N° 374-2017-VIVIENDA que aprueba la Política de Seguridad de la Información del Ministerio de Vivienda, Construcción y Saneamiento.

4.15 Resolución Ministerial N° 119-2018-PCM, modificado por Resolución Ministerial N° 087-2019-PCM, que aprueba el Comité de Gobierno Digital, así como se establecen las funciones del mismo, su alcance, y los lineamientos de gestión y planificación en Gobierno Digital

4.16 Directiva N° 005-2003-INEI/DTNP "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública", aprobada por Resolución Jefatural N° 088-2003-INEI.

4.17 Directiva General N° 001-2022-VIVIENDA-DM, "Disposiciones para la formulación, aprobación, modificación y derogación de directivas y lineamientos en el Ministerio de Vivienda, Construcción y Saneamiento".

V. DISPOSICIONES GENERALES

5.1 Siglas y Acrónimos

5.1.1.	CC	: Con copia
5.1.2.	CCO	: Con copia oculta
5.1.3.	MVCS	: Ministerio de Vivienda, Construcción y Saneamiento
5.1.4.	PNSU	: Programa Nacional de Saneamiento Urbano
5.1.5.	PNSR	: Programa Nacional de Saneamiento Rural
5.1.6.	PASLC	: Programa Agua Segura para Lima y Callao
5.1.7.	OACP	: Oficina de Abastecimiento y Control Patrimonial.
5.1.8.	OGA	: Oficina General de Administración
5.1.9.	OGC	: Oficina General de Comunicaciones
5.1.10.	OGEI	: Oficina General de Estadística e Informática
5.1.11.	OGGRH	: Oficina General de Gestión de Recursos Humanos
5.1.12.	OTI	: Oficina de Tecnología de la Información.
5.1.13.	PCM	: Presidencia del Consejo de Ministros.
5.1.14.	STPAD	: Secretaría Técnica de Procedimiento Administrativo Disciplinario.
5.1.15.	SITRAD	: Sistema Integrado de Trámite Documentario.
5.1.16.	SG	: Secretaria General

5.2 Definiciones

Para efectos de la presente disposición, se entiende por:

5.2.1. **Backup**: Copia de seguridad, respaldo, copia de respaldo, copia de reserva (del inglés backup) en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

5.2.2. **Cookies**: Archivo de pequeño tamaño enviado por un sitio web y almacenado en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador.

5.2.3. **Correo electrónico:** Servicio tecnológico que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos.

5.2.4. **Doble Factor de autenticación (2FA):** Ofrece una capa de seguridad adicional para los archivos en línea, lo cual mantiene tus datos confidenciales escudados frente a ciber amenazas potenciales.

5.2.5. **Flyers:** Volante o folleto de pequeño tamaño que contiene un mensaje de tipo comercial.

5.2.6. **Hacking:** Búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes.

5.2.7. **Información:** Datos que pueden ser procesados, distribuidos, almacenados y representados en cualquier medio electrónico, digital, óptico, magnético, impreso u otros, que son el elemento fundamental de los activos de información.

5.2.8. **Malware:** Programa o software malicioso, maligno, malintencionado. En inglés malware, badware o código maligno, hacen referencia a cualquier tipo de software malicioso diseñado para infiltrarse en sistema informáticos y causar daños de diversas formas, como ralentizar el equipo, recopilar información de los usuarios o redirigir tráfico web sitios no deseados sin el conocimiento del usuario.

5.2.9. **Navegador web:** Software, aplicación o programa que permite el acceso a la web, interpretando la información de distintos tipos de archivos y sitios web para que estos puedan ser vistos.

5.2.10. **Oficial de Seguridad de la Información:** Responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la entidad.

5.2.11. **Phishing:** Métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

5.2.12. **Programas:** Se hace referencia al Programa Nacional de Saneamiento Urbano (PNSU), Programa Nacional de Saneamiento Rural (PNSR), y Programa Agua Segura para Lima y Callao (PASLC).

5.2.13. **SMTP Relay:** Es el protocolo de envíos más utilizado en la actualidad y utilizado exclusivamente para la entrega de grandes volúmenes de mensajes.

5.2.14. **Software:** Equipamiento o soporte lógico de una computadora que hacen posible la realización de tareas específicas.

5.2.15. **Spam:** Programa escrito intencionalmente para auto instalarse en la computadora de un usuario sin el conocimiento o permiso de éste. Se comporta como un programa que infecta o ataca a los archivos del sistema y del usuario.

5.2.16. **Streaming:** Es la distribución digital de contenido multimedia a través de una red de computadoras, de manera que el usuario utiliza el producto a la vez que se descarga.

5.2.17. **Usuario:** Persona que realiza determinada labor dentro de la entidad y a quién se le asigna una identificación digital para acceder a ciertos servicios informáticos disponibles.

5.2.18. **Virus:** Es un programa que puede infectar o contaminar otros programas al modificarlos para incluir una copia de sí mismo. El código viral es típicamente malicioso y perjudicial para la integridad de la información o del sistema.

5.3 Sobre el uso del Correo Electrónico

a) El uso del correo electrónico, es exclusivamente para acciones, funciones o actividades relacionadas a todo/a servidor/a civil, practicantes y prestadores de servicios contratados del MVCS y sus Programas.

b) La OTI de la OGEI, o la que haga sus veces en los programas, es responsable de la administración de la plataforma tecnológica de correo electrónico en el MVCS.

c) La OTI de la OGEI, o la que haga sus veces en los programas, no administra la información que contiene un correo electrónico, no tiene conocimiento de los mensajes o información contenida en este.

d) La OTI de la OGEI, o la que haga sus veces en los programas, en cumplimiento de la NTP ISO/IEC 27001:2022 y en salvaguarda de la seguridad de la información, tiene la función de garantizar, monitorear, controlar y administrar la plataforma del servicio correo electrónico.

e) El correo electrónico es para uso exclusivo y bajo responsabilidad del servidor/a civil y/o practicante en el MVCS y programas a quién se le asigna la cuenta.

f) Toda información o contenido que sea transmitido por las cuentas de correo, son responsabilidad exclusiva del titular de la cuenta, por lo que dichos contenidos no reflejan las preferencias o ideas del MVCS o Programas.

g) El uso de la característica de doble autenticación para el servicio de correo electrónico es de uso obligatorio y es responsabilidad del usuario solicitar su activación y responsabilidad de la OTI de la OGEI, o la que haga sus veces en los programas, su implementación en la plataforma de correo.

VI. DISPOSICIONES ESPECÍFICAS

6.1 AUTORIZACIÓN Y CREACIÓN DEL CORREO ELECTRÓNICO

6.1.1 Autorización de solicitar correo

a) La Oficina General de Gestión de Recursos Humanos (OGGRH), o la que haga sus veces en los programas, solicita la creación de cuentas de correo electrónico para servidores/as civiles y practicantes indicando el Órgano y/o Unidad Orgánica a la que pertenece, así como su modificación. La solicitud se realiza a través de correo electrónico: mesadeservicios@vivienda.gob.pe, o la que haga sus veces en los

programas, quienes finalmente definen el nombre del usuario teniendo en cuenta lo señalado en el numeral 6.1.2 de la presente Directiva.

b) La Oficina General de Administración a través de la Oficina de Abastecimiento y Control Patrimonial (OACP) de la Oficina de Administración (OGA), o la que haga sus veces en los programas, solicita la creación de cuentas de correo electrónico para servicios contratados por el MVCS o programas, indicando el Órgano y/o Unidad Orgánica donde se ejecutará el servicio, así como la fecha inicio y fecha fin del servicio.

c) La solicitud de creación de cuenta de correo electrónico por parte de OGGRH y OACP, o la que haga sus veces en los programas, se realiza a través de correo electrónico, el cual será remitido a la mesadeservicios@vivienda.gob.pe, quienes finalmente definen el nombre del usuario teniendo en cuenta lo señalado en el numeral 6.1.2 de la presente Directiva.

d) El Director/a General (MVCS), o la que haga sus veces en los programas, puede solicitar la creación de una cuenta especial para una actividad específica, este requerimiento deberá ser solicitado por el Sistema de Trámite Documentario (SITRAD) u otro análogo, señalando al órgano y/o unidad orgánica, así como al responsable de la administración de la cuenta y el tiempo de vigencia de la cuenta solicitada hasta un máximo de 365 días calendario, renovables.

e) La designación de personal que sea publicada en el Diario Oficial El Peruano, autoriza a la OTI de la OGEI, la creación de cuentas de correo electrónico del personal designado.

f) Al recibir una cuenta de correo, el usuario acepta las condiciones de uso y responsabilidades establecidas en la presente Directiva.

6.1.2 De la creación de correos

a) La OTI de la OGEI crea las cuentas de correo electrónico en la plataforma previo cumplimiento de lo indicado en el numeral 6.1.1.

b) La nomenclatura de la cuenta de correo electrónico institucional para personal está formada por la letra inicial del primer nombre del usuario seguido inmediatamente del apellido paterno, ligado con el símbolo @ al nombre de dominio del MVCS.

Ejemplo:	***Cuenta de Correo***	***@nombre-Dominio***
	dfrancia	*@vivienda.gob.pe*

c) En caso de existir dos cuentas similares, el administrador de la plataforma de correo electrónico de la OTI, procede a incluir el primer carácter (la primera letra) del segundo apellido de la persona recientemente incorporada. Y si persiste la similitud, se coloca el primer nombre completo seguido por un punto y finalizando con el primer apellido completo.

Ejemplo:	***Cuenta de Correo***	***@nombre-Dominio***
	dfranciap	*@vivienda.gob.pe*
	diego.francia	*@vivienda.gob.pe*

d) La nomenclatura de la cuenta de correo electrónico institucional para servicios contratados, esta se creará con la siguiente estructura:

Ejemplo:	***Cuenta de Correo***	***@nombre-Dominio***
MVCS_DireccionGeneral_inicialesNombreCompleto		*@viviendaext.pe*

e) La nomenclatura de cuentas especiales de correo electrónico institucional para una actividad específica se creará con la siguiente estructura:

Ejemplo:	***Cuenta especial***	***@nombre-Dominio***
	denuncias	*@vivienda.gob.pe*

6.2 USO DEL CORREO ELECTRÓNICO

6.2.1 Uso de contraseñas

Toda contraseña generada debe ser de difícil deducción para otras personas y fácil de recordar para el usuario, debiendo cumplir con las siguientes características:

a) Tener como mínimo ocho (8) caracteres alfanuméricos incluyendo una mezcla de letras mayúsculas y minúsculas, números y caracteres especiales (!#$%&*/¿[]{}<>), además utilizar acrónimos o frases que lo ayuden a memorizar las contraseñas.

b) La contraseña tendrá una vigencia máxima de 90 días calendario, finalizando este periodo el usuario deberá realizar el cambio correspondiente.

c) No deben ser susceptibles a ataques de diccionario, es decir, que no incluya palabras que podrían ser encontradas en un diccionario.

6.2.2 Uso de doble factor de autenticación

Toda cuenta de correo electrónico debe hacer uso del doble factor de autenticación, el cual añade una capa adicional de seguridad a la cuenta.

6.2.3 Lectura de correo

El correo electrónico es un medio de comunicación oficial del MVCS y programas. Es responsabilidad del usuario la lectura diaria.

6.2.4 Envío de correo

a) Es obligatorio utilizar el campo “asunto”. En dicho campo se expresa brevemente el contenido y/o tema del mensaje en mención.

b) Cuando se envíe correo, se debe conocer al destinatario, a menos que sea un asunto oficial que lo involucre, con el objetivo de que los correos con dominio @vivienda.gob.pe y @viviendaext.pe no sean considerados SPAM o correo no deseado.

c) Se encuentra prohibido el envío de correos a todo el MVCS o a todos los programas, a menos que sea un asunto oficial; en ese caso solo las oficinas autorizadas para este fin pueden realizar los envíos de mensajes,

además para ocultar las direcciones de los destinatarios, se debe añadir al campo “Cco” (copia oculta).

d) Antes de enviar el mensaje, el usuario debe revisar el texto que lo compone y los destinatarios, con el fin de corregir posibles errores de ortografía, forma y fondo.

e) Cuando se desee responder o acusar recibo usar las siguientes opciones:

i. **“Responder”:** Da respuesta al mensaje de correo electrónico solo al remitente y no a otros destinatarios que se encuentren en el campo “CC” en el mensaje de correo.

ii. **“Responder a todos”:** Da respuesta al mensaje de correo electrónico al remitente y copia a todos los destinatarios que se encuentran en el campo “CC”, por lo que todos tomarán conocimiento de su respuesta.

6.2.5 Reenvío de mensajes

a) Para el reenvío de un mensaje, se incluye el mensaje original de ser el caso, a fin que el destinatario conozca el contexto en que se está dando el mensaje que recibe.

b) Está prohibido el envío o reenvío de mensajes tipo Spam, publicitarios o cadenas.

6.2.6 Firma del correo electrónico

a) El diseño de la firma de correo electrónico es elaborado por la Oficina General de Comunicaciones (en adelante OGC) a través del “Manual de Identidad Gráfica del Ministerio de Vivienda, Construcción y Saneamiento”, aprobado con Resolución Ministerial N° 199-2023-VIVIENDA.

b) El(a) coordinador(a) administrativo(a) de cada Dirección/Oficina/Programa debe enviar la lista de los/las servidores/as civiles con los datos que establece el diseño (Pág. 36 del Manual de Identidad) que corresponden a: nombre, apellido, cargo, oficina, teléfono y anexo. Dicha solicitud debe ser dirigida mediante correo electrónico al(a) Director(a) de la oficina de Imagen Institucional o la que haga sus veces en los programas.

c) Todo mensaje a ser enviado incluye la firma respectiva. El usuario es responsable de incluir la firma automática en todos los mensajes que envíe y/o responda.

6.2.7 Tamaño de los mensajes

a) El tamaño máximo de los mensajes está predeterminado por la plataforma de correo que contrate el MVCS y los programas (actualmente 25MB).

b) En caso el archivo a adjuntar supere esa capacidad, se debe enviar como vínculo de Google Drive.

6.2.8 Vigencia de la cuenta de correo

La cuenta de correo electrónico se mantendrá "vigente" hasta el término de la relación laboral, conclusión del convenio de modalidad formativa o la prestación del servicio correspondiente, lo que debe ser -obligatoriamente- comunicado por la OGGRH y/o el fin del servicio contratado e indicado por la Oficina de Abastecimiento y Control Patrimonial (OACP) o la que haga sus veces en los programas en el literal b) del subnumeral 6.1.1 del numeral 6.1; transcurrido dicho plazo la OTI o la que haga sus veces en los programas eliminará al mismo.

6.2.9 Listas de correos

Sólo está permitido suscribirse a listas de interés absolutamente necesarias e indispensables para el adecuado ejercicio de la función institucional, con la finalidad de evitar saturación en la recepción de mensajes. La OGEI a través de la OTI o la que haga sus veces en los programas permanentemente realiza un control de las listas de interés a las que se encuentren suscritos los usuarios, para la permanencia en dicha lista o el bloqueo de mensajes de la misma.

Está prohibido marcar como SPAM o correo no deseado cuentas del dominio @vivienda.gob.pe y/o @viviendaext.pe

6.2.10 Correo institucional desde fuera de las instalaciones del MVCS

a) El acceso al servicio de correo electrónico está disponible en cualquier lugar que disponga de un acceso a internet y está garantizado a través de su plataforma móvil o Web.

b) El acceso a las cuentas de correo institucional, podrá ser a través de cualquier navegador Web, dispositivos móviles, así como de las aplicaciones de escritorio compatibles con la plataforma de correo establecida.

c) Si se inicia sesión en un navegador Web de un dispositivo de uso público, debe iniciar sesión en modo privado o incógnito para evitar que datos privados como contraseñas o datos personales sean almacenados en el historial o cookies del equipo; y cerrar sesión de la cuenta al terminar sus actividades.

d) En caso de pérdida de un dispositivo móvil vinculado a su cuenta de correo electrónico institucional, deberá hacer el cambio de contraseña del correo electrónico o comunicarlo a las OTI o la que haga sus veces en los programas a través del correo electrónico.

6.2.11 Seguridad del correo electrónico

a) La OGEI o la que haga sus veces en los programas a través de su proveedor de servicio de correo electrónico, es la encargada de establecer medidas de seguridad y respaldo del sistema de mensajería que permitan ofrecer una continuidad en el servicio.

b) Se sugiere no hacer uso de aplicaciones de terceros o sin licencia, ajenas a las recomendadas por el proveedor del servicio de correo electrónico.

6.2.12 Validez oficial del correo electrónico

a) Al ser el correo electrónico institucional la herramienta dispuesta por el MVCS como medio de comunicación oficial, se prohíbe el uso de correos personales con el fin de establecer o transferir información institucional.

b) Toda comunicación masiva oficial es realizada por las oficinas autorizadas para este fin, esto incluye la difusión de normas, directivas, reglamentos, procedimientos, flyers, etc.

6.2.13 Ausencia

Los usuarios con ausencia programada del MVCS o programas que supere(n) tres (3) días (vacaciones u otro motivo), deberán configurar una respuesta para notificar -automáticamente- a los demás su ausencia, consignando fecha de retorno, funcionario alterno de contacto, para que el remitente pueda -oportunamente- derivar su comunicación a otras instancias hasta su retorno.

6.2.14 Privacidad de los mensajes

El correo electrónico, desde el punto de vista del contenido del mensaje, debe ser considerado como de dominio público o de mensajería insegura. Eso significa que no se debe incluir contraseñas u otra información confidencial, a menos que esta se encuentre en un archivo adjunto encriptado.

6.2.15 Controles

a) Verificar los remitentes antes de abrir un correo electrónico. En caso de sospecha de suplantación, contactar con el remitente por otro medio para confirmar.

b) En caso de dudar o sospechar de la autenticidad de un correo electrónico porque el mensaje presenta cambios de aspecto inusuales, llamadas a la acción urgentes o solicitud de credenciales de acceso a una web o aplicación (cuenta bancaria, accesos, etc.), se recomienda no hacer click en los enlaces ni abrir archivos adjuntos, no introducir datos personales o bancarios, contactar con la empresa por otros medios para verificar la verosimilitud del mensaje o eliminar el correo sospechoso.

c) El MVCS o programas nunca:

   i. Solicita datos de acceso (usuario y/o contraseñas).
   ii. Solicita verificar su cuenta o datos.
   iii. Ofrece ampliación del espacio del correo.

d) En caso de sospechar de la autenticidad de un correo electrónico que contiene archivos adjuntos y/o proviene de remitentes desconocidos; no descargar ni abrir el correo y, seguidamente, comunicar a la OTI o la que haga sus veces en los programas, a través del correo electrónico.

e) En el supuesto de recibir mensajes de publicidad, marcar el mensaje como spam y/o eliminar.

6.2.16 Envío de correos a través de aplicaciones informáticas o dispositivo electrónico

El SMTP (Simple Mail Transfer Protocol) Relay debe ser utilizado para aplicaciones o dispositivos electrónicos, los cuales necesitan enrutar mensajes salientes.

6.2.17 Grupos de correos

a) Para la creación de grupos de correo, el usuario deberá solicitarlo a través de la mesa de ayuda o la que haga sus veces en los programas, adjuntando lo siguiente:

   i. Nombre del grupo
   ii. Descripción del grupo
   iii. Lista de correos a incorporar al grupo
   iv. Tipo de permisos:
      - Grupo Cerrado: Para comunicación Interna
      - Grupo Abierto: Permite comunicación externa

b) Para poder enviar mensajes mediante una dirección de correo electrónico de grupo, deberá solicitar su configuración a la OTI o la que haga sus veces en los programas.

6.2.18 Prohibiciones

Queda prohibido:

a) Facilitar y ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas.

b) Suplantar la identidad de otro usuario.

c) Utilizar otra cuenta de correo electrónico institucional que no sea la asignada al usuario.

d) La asignación de más de una cuenta de correo por usuario.

e) Instalar algún servicio de correo electrónico o cualquier tecnología de envío y recepción de correo electrónico en la red del MVCS o programas distinta al correo institucional.

f) Obstruir el acceso al servicio de correo electrónico de un usuario, sin la autorización escrita o electrónica de la Oficina General de Gestión de Recursos Humanos o la que haga sus veces en los programas según el tipo de contrato correspondiente.

g) Difundir contenidos inadecuados, como mensajes: con contenidos impropios y/o lesivos a la moral, contra la reputación de personas y las buenas costumbres, actividades políticas partidarias. Asimismo, todo lo que constituya complicidad con hechos delictivos, por ejemplo: apología del terrorismo, uso y/o distribución de programas piratas, amenazas, estafas, esquemas de enriquecimiento piramidal, todo tipo de pornografía, planificación o ejecución de estafas (phishing), spam, malware o código hostil (virus) en general, difundir información a terceros en perjuicio del MVCS o programas.

h) Utilizar el correo electrónico para cualquier propósito comercial o financiero ajeno al MVCS o programas.

i) Propagar información y/o documentos de trabajo a personas ajenas al MVCS o programas, con fines ajenos al desempeño de su función.

j) Enviar mensajes que comprometan la información estratégica del MVCS o programas o contravengan las leyes.

k) Utilizar el correo electrónico para intimidar, insultar, hostilizar o acosar a los usuarios del MVCS o programas.

6.2.19 Backup o Respaldo de Correo Electrónico

6.2.19.1. Cuentas de correo electrónico sin relación Contractual

a) Posterior a la vigencia de la cuenta de correo (6.2.8) y previo a la eliminación de la cuenta de correo, la OTI de la OGEI o la que haga sus veces en los programas, realiza una copia de respaldo (backup) completa de la cuenta de correo, que comprende todos los correos enviados y recibidos desde el inicio de la relación contractual del usuario hasta el fin de la misma, usando la herramienta de backup disponible.

b) Eliminada la cuenta de correo electrónico no es posible realizar backup de fechas acotadas sin manipular la data del backup, por lo que pedidos de copia de backup de fechas acotadas serán atendidos con copias fiel de backups que la OTI de la OGEI, o la que haga sus veces en los programas, custodia y que fueron realizados con la herramienta de backup.

c) La OTI de la OGEI, o la que haga sus veces en los programas, en el marco de las funciones que le han sido asignadas mediante el vigente Reglamento de Organización y funciones – ROF del Ministerio de Vivienda, Construcción y Saneamiento – MVCS, custodia la copia de respaldo (Backup) de todas las cuentas de correos que tuvieron relación contractual o prestaron servicios en el MVCS o programas.

d) El backup de la cuenta de correo está disponible en el MVCS o programas ciento veinte (120) días calendario, contados desde la fecha del vencimiento de la relación contractual. Transcurrido dicho plazo y en caso de no contar con recursos disponibles para su almacenamiento, previo informe técnico la OTI de la OGEI, o la que haga sus veces en los programas, elimina la copia de respaldo que custodia.

e) Para acceder a una copia de los backup de correos electrónicos que la OTI de la OGEI, o la que haga sus veces en los programas, custodia es necesario cumplir con los siguientes supuestos:

e.1 Pedido Fiscal, Contraloría, Procuraduría General del Estado y/o Juez/a: La atención se realizará a través de La Procuraduría Pública del MVCS o la que haga sus veces en los programas en el marco de la normativa y procedimientos

vigentes y en cumplimiento de la Ley N° 27806 “Ley de Transparencia y Acceso a la Información Pública.

En atención a lo indicado y sin perjuicio a ello, el Titular de la Procuraduría Pública del MVCS o la que haga sus veces en los programas podrá solicitar a la OGEI, o la que haga sus veces en los programas, una copia fiel del backup de correo electrónico que como área técnica custodia.

e.2 Pedido STPAD: En el marco de una investigación la STPAD solicitará mediante trámite documentario a La OGEI o la que haga sus veces en los programas una copia del backup de correo electrónico que la OGEI o la que haga sus veces en los programas custodia y proceder en el marco de la normativa y procedimientos vigentes.

e.3 Pedido de Acceso a la Información Pública: La atención lo realizará el Órgano o Unidad Orgánica del MVCS o programa donde el excolaborador prestó servicios, para lo cual el titular del Órgano o Unidad Orgánica deberá solicitar a la OGEI, o la que haga sus veces en los programas, una copia del backup de correo electrónico que la OGEI o la que haga sus veces en los programas custodia y proceder en el marco de la normativa y procedimientos vigentes y en cumplimiento de la Ley N° 27806 “Ley de Transparencia y Acceso a la Información Pública.

6.2.19.2 Cuentas de correo electrónico con relación contractual

a) El backup de un correo electrónico es realizado por el usuario usando la herramienta **TAKEOUT**[1] de Google, en caso de requerir apoyo tecnológico, este debe ser solicitado a la OTI de la OGEI, o la que haga sus veces en los programas.

b) Estos backup(s) pueden ser acotados por fechas y los debe realizar el usuario que tenga la cuenta de correo asignada.

c) Para la entrega de una copia de los backup de correos electrónicos de los usuarios vigentes y que prestan servicios en el MVCS o programas, es necesario cumplir con los siguientes supuestos:

c.1. Pedido Fiscal, Contraloría, Pedido de Acceso a la Información Pública y/o Juez/a: La atención lo realizará el Órgano o Unidad Orgánica del MVCS o programas donde el colaborador presta servicios en el marco de la normativa y procedimientos vigentes y en el marco de la Ley N° 27806 “Ley de Transparencia y Acceso a la Información Pública, para lo cual podrá solicitar apoyo tecnológico a la OTI de la OGEI, o la que haga sus veces en los programas.

c.2. Pedido STPAD: En el marco de una investigación la STPAD solicitará mediante trámite documentario a la OGEI, o la que haga sus veces en los programas, la generación del backup

[1] https://support.google.com/accounts/answer/3024190?hl=es

de correo electrónico del servidor/a civil investigado en el marco de la normativa y procedimientos vigentes.

VII. RESPONSABILIDAD

7.1 La OTI de la OGEI y el Oficial de Seguridad de la Información y quién haga sus veces en los programas, son los encargados de velar por el cumplimiento administrativo y técnico, respectivamente, de lo dispuesto en la presente Directiva.

7.2 Los usuarios del MVCS (Órganos, Unidades Orgánicas) y programas que tengan acceso a los servicios del correo electrónico en el MVCS, desarrollan sus actividades en cumplimiento de los principios éticos y valores en aplicación del Código de Ética de la Función Pública.

VIII. DISPOSICIONES COMPLEMENTARIAS

8.1 El usuario que recibe algún correo no deseado, se comunica a la OTI de la OGEI, o la que haga sus veces en los programas, a través de la Mesa de Servicios mesadeservicios@vivienda.gob.pe o al correo infosec@vivienda.gob.pe, a fin de evitar que dicho remitente vuelva a tomar contacto con el usuario.

8.2 La OGGRH o la que haga sus veces en los programas deberá notificar el inicio de labores o el desarrollo de la modalidad formativa de los usuarios del MVCS o programas, en un plazo máximo de 24 horas para la activación de las cuentas de correo electrónico respectivas.

8.3 La OGGRH o la que haga sus veces en los programas deberá notificar cada cese o la conclusión del convenio de la modalidad formativa, en un plazo máximo de 48 horas para la desactivación de las cuentas de correo electrónico respectivas.

8.4 La OGEI o la que haga sus veces en los programas es responsable de la difusión de la presente Directiva y que los usuarios del MVCS y programas cumplan con lo dispuesto en ella.

IX. ANEXOS

No Aplica