Trujillo, 23 de Agosto del 2026

OFICIO MULTIPLE N° 000621-2026-GRLL-GGR-GRE

Señores:
Jesús Cosme Joaquin Ruiz
Director
Unidad de Gestión Educativa Local de Ascope

Eli Hebert Rodríguez Mantilla
Director
Unidad de Gestión Educativa Local de Bolívar

Carlos Alberto López Perez
Director
Unidad de Gestión Educativa Local de Chepén

Carlos Alfredo Chang Jiménez
Director
Unidad de Gestión Educativa Local La Esperanza

Gregorio Marcelino Marín Huamán
Director
Unidad de Gestión Educativa Local de Gran Chimú

María Jesus Alcántara Castro
Directora
Unidad de Gestión Educativa Local de Julcán

Andrés Lino Aguilar Acevedo
Director
Unidad de Gestión Educativa Local de Otuzco

Roberto Carlos Asmat Castro
Director
Unidad de Gestión Educativa Local de El Porvenir

Erlinda Elena Zárate Vidal
Directora
Unidad de Gestión Educativa Local de Pacasmayo

Toribia Iraida Medina Rosas
Directora
Unidad de Gestión Educativa Local de Pataz

Jacqueline Akemi Alvarado Lázaro
Directora
Unidad de Gestión Educativa Local de Santiago de Chuco

Miller Nicolás Contreras Morales
Director
Unidad de Gestión Educativa Local de Sánchez Carrión

Rocio Elizabeth Rebaza Blas
Directora
Unidad de Gestión Educativa Local N° 03 Trujillo Nor Oeste

Jorge Alberto Asmat Castro
Director
Unidad de Gestión Educativa Local N° 04 Trujillo Sur Este

Hernández Heder Ticlia Murga
Director
Unidad de Gestión Educativa Local de Virú

Crhistian Delgado Monteagudo
Director
Colegio Militar Ramon Castilla
Presente. -

Asunto : Dispone adoptar y reforzar medidas de seguridad para el acceso a equipos informáticos, sistemas, plataformas y cuentas institucionales.

Me dirijo a ustedes con relación a la **necesidad de fortalecer las medidas preventivas de seguridad de la información en las Unidades de Gestión Educativa Local**, particularmente respecto del acceso y utilización de computadoras, correos electrónicos institucionales, sistemas administrativos, plataformas digitales, aplicativos y demás recursos tecnológicos empleados para el cumplimiento de las funciones institucionales.

Los usuarios, contraseñas, códigos de verificación y demás mecanismos de autenticación permiten identificar al servidor que accede a un determinado sistema y, dependiendo de los permisos asignados, posibilitan consultar, registrar, modificar, procesar o remitir información institucional. Por esta razón, su custodia no constituye una formalidad, sino una medida necesaria para prevenir accesos no autorizados, suplantaciones de identidad, alteración o pérdida de información y otras situaciones que puedan comprometer la seguridad de la entidad.

En atención a ello, **SE DISPONE** que, bajo responsabilidad de la Dirección de cada UGEL, se adopten y hagan de conocimiento obligatorio de todo el personal las siguientes medidas:

1. **Mantener bajo estricta reserva los usuarios, contraseñas y demás credenciales de acceso** a correos electrónicos, computadoras, sistemas administrativos, plataformas institucionales, aplicativos y servicios digitales utilizados para el ejercicio de sus funciones.
2. **No compartir, prestar, ceder ni proporcionar credenciales de acceso a terceras personas**, incluyendo otros servidores de la propia entidad. Las cuentas personales o individualizadas deberán ser utilizadas exclusivamente por el servidor al cual fueron asignadas.
3. Utilizar **contraseñas robustas y diferenciadas**, evitando nombres, fechas, números de documentos u otros datos fácilmente identificables, así como la reutilización de una misma contraseña para cuentas institucionales y personales.
4. Disponer el **cambio inmediato de contraseña** cuando exista sospecha de que esta haya sido conocida, expuesta o utilizada por terceros, o cuando se detecten accesos, comunicaciones, modificaciones u operaciones que el titular de la cuenta no reconozca.
5. Implementar o activar, cuando la plataforma lo permita, **mecanismos de autenticación multifactor**, principalmente en cuentas y sistemas que permitan acceder a información institucional o realizar operaciones administrativas.
6. **Bloquear el equipo o cerrar temporalmente la sesión cuando el servidor se retire de su puesto de trabajo**, aun por periodos breves, y cerrar las sesiones de los sistemas y plataformas al concluir la jornada laboral.

7. Impedir que personas no autorizadas utilicen los equipos informáticos institucionales o accedan a información contenida en ellos. Del mismo modo, deberá evitarse la instalación de programas, aplicaciones, extensiones o archivos cuya procedencia o seguridad no haya sido previamente verificada.
8. **Extremar las medidas de prevención frente a correos electrónicos, mensajes, enlaces, archivos adjuntos, códigos QR o formularios sospechosos**, especialmente aquellos que soliciten actualizar contraseñas, validar cuentas, ingresar códigos de seguridad, proporcionar información personal o institucional, efectuar pagos o realizar operaciones no habituales.
9. **No almacenar contraseñas o credenciales en lugares visibles o desprotegidos**, tales como notas adheridas a los equipos, agendas de fácil acceso, documentos de texto sin protección o archivos compartidos.
10. Evitar almacenar, trasladar, reproducir o remitir **información institucional mediante correos electrónicos personales, dispositivos externos, servicios de almacenamiento o plataformas no autorizadas**, particularmente cuando se trate de información personal, administrativa, financiera, laboral o aquella cuyo acceso se encuentre restringido.
11. Disponer que cualquier **pérdida o sustracción de equipos, intento de acceso no autorizado, suplantación de identidad, correo fraudulento, infección por software malicioso, alteración de archivos, exposición de contraseñas, filtración de información o actividad informática sospechosa** sea comunicada inmediatamente al responsable o área competente de la UGEL para la adopción de las medidas de contención y seguridad correspondientes.
12. Revisar periódicamente los **perfiles, permisos y niveles de acceso** asignados al personal, procurando que cada servidor cuente únicamente con aquellos que resulten necesarios para el cumplimiento de sus funciones.
13. Cuando se produzca el **cese, término de contrato, desplazamiento, rotación, reasignación, destaque, vacaciones u otra circunstancia que determine que un servidor deje de requerir determinados accesos**, deberán adoptarse oportunamente las acciones para suspender, cancelar o modificar las credenciales y permisos correspondientes.
14. Evitar que las credenciales pertenecientes a servidores que hayan cesado o dejado determinado puesto **continúen activas o sean utilizadas por sus reemplazantes**. Cuando corresponda habilitar acceso al nuevo responsable, deberá gestionarse una credencial propia o efectuar formalmente la modificación que permita identificar al usuario autorizado.
15. Mantener actualizados los sistemas operativos, programas de protección y demás componentes de seguridad de los equipos institucionales, conforme a las disposiciones y procedimientos establecidos por el área responsable de tecnologías de la información.

Asimismo, se deberá orientar al personal sobre los riesgos asociados a la **ingeniería social, phishing, suplantación de identidad y apropiación de credenciales**, enfatizando que ninguna solicitud inusual de contraseña, código de autenticación o información reservada debe atenderse sin verificar previamente la identidad del solicitante y la legitimidad del requerimiento.

Cada director de UGEL deberá disponer que el responsable o área competente en tecnologías de la información **evalúe las condiciones de seguridad de los equipos, cuentas, redes, sistemas y plataformas bajo su administración**, identificando accesos que deban ser actualizados o cancelados y adoptando las acciones correctivas que correspondan dentro del ámbito de sus competencias.

Del mismo modo, deberá asegurarse que la asignación, modificación y cancelación de accesos se encuentre vinculada a las funciones efectivamente desempeñadas por cada servidor,

evitando cuentas compartidas, credenciales genéricas cuando técnicamente puedan individualizarse los accesos, así como la permanencia injustificada de permisos correspondientes a funciones que el servidor ya no ejerce.

En consecuencia, **se DISPONE la difusión inmediata del presente oficio a todo el personal de su jurisdicción y supervisar directamente su cumplimiento**, adoptando las medidas administrativas y técnicas que correspondan para proteger la información y los recursos tecnológicos institucionales.

La seguridad de los sistemas y de la información institucional constituye una responsabilidad que involucra tanto a quienes administran los recursos tecnológicos como a cada servidor que cuenta con credenciales y permisos de acceso. Por ello, cualquier incidente o vulnerabilidad detectada deberá ser atendido oportunamente y comunicado por los canales institucionales correspondientes.

Hago propicia la oportunidad para expresarles los sentimientos de mi especial consideración.

Atentamente,

Documento firmado digitalmente por
RUFINO RODRIGUEZ ROMAN
GERENTE
GERENCIA REGIONAL DE EDUCACIÓN
GOBIERNO REGIONAL LA LIBERTAD