El uso indebido de cualquiera de estos tres elementos está prohibido e incluye:

a. Intentar instalar u operar puntos de acceso inalámbricos (Access Point) conectados a la red cableada de la Organización sin la autorización de la gerencia.

b. Intentar modificar, reubicar o sustraer del lugar donde han sido instalados o configurados, equipos de cómputo, software información o periféricos sin la debida autorización.

c. Acceder sin la debida autorización de la Organización a través del soporte técnico, mediante computadores, celulares y otros dispositivos, software, información o redes de la Organización, a recursos externos o internos que pertenezcan a la organización (bases de datos, sistemas de información, redes externas o de investigación a las cuales esté vinculada.)

d. Enviar o trasmitir por cualquier medio (Internet, correo, USB, medio impreso, cd, etc.), Información privada de la organización a personas que no le competen.

e. Interferir sin autorización el acceso de otros usuarios a los recursos de los sistemas de información de la Organización.

f. Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.

g. Utilizar los sistemas de información para propósitos ilegales o no autorizados (externos e internos).

h. Enviar cualquier comunicación electrónica fraudulenta.

i. Violar cualquier licencia de software o derechos de autor, incluyendo la copia o distribución de software protegido legalmente sin la autorización escrita del propietario del software.

j. Usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores.

k. Usar las comunicaciones electrónicas para acosar o amenazar a los usuarios de la Organización o externos, de alguna manera que sin razón interfiera con el buen desempeño de las actividades de todo el personal perteneciente a la Organización.

l. Usar las comunicaciones electrónicas para revelar información privada sin el permiso explícito del dueño.

m. Leer la información o archivos de otros usuarios sin su permiso.

n. Alterar o falsificar de manera fraudulenta los registros de la Organización (incluyendo registros computarizados, permisos, documentos de identificación, u otros documentos o propiedades).

o. Usar las comunicaciones electrónicas para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.

p. Usar las comunicaciones electrónicas para apropiarse de los documentos de otros usuarios.

q. Lanzar cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil o destructiva.

r. Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un computador de la Organización.

s. Transportar o almacenar material con derechos de propiedad o material nocivo usando las redes de la Organización.

t. Utilizar cualquier sistema de información de la Organización para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material obsceno.

u. Violar cualquier ley o regulación nacional respecto al uso de sistemas de información.

v. Instalar o usar software de espionaje, monitoreo de tráfico o programas maliciosos en la Red.

w. Introducir cualquier tipo de programa o instalar cualquier software sin la autorización por escrito de la gerencia de ODP & CIA S.A.S.

x. Efectuar violaciones a la seguridad o interrupciones de la comunicación de la red. Las violaciones de la seguridad incluyen “sniffer” “floodeos” “Packet Spoofing”, negación del servicio (DOS), manipulación de ruteo, etc.

y. Evitar o interceptar la autenticación de cualquier usuario por cualquier método. Usar cualquier método (exploits, scripts, comandos) para acceder a recursos a los que no se tiene acceso a áreas protegidas.

ORLANDO DONADO POLO
REPRESENTANTE LEGAL

Última revisión: enero 14 de 2026