



PERÚ

Ministerio
de Salud

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"

SOLICITUD DE ACCESOS PARA USB/CD/DVD

DATOS DEL USUARIO SOLICITANTE

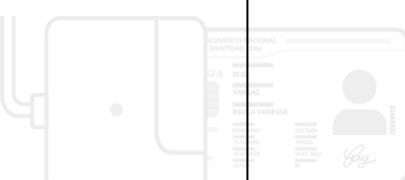
Apellidos y nombres _____ Fecha _____
Cuenta de usuario _____ DNI Nº _____
Dirección/Oficina General _____
Cargo _____ Teléfono / Anexo: _____
Condición laboral _____
Periodo de uso: Desde _____ hasta _____

Sustento para acceso al puerto USB/ CD/DVD

Dispositivo de Almacenamiento

DECLARACION DE RESPONSABILIDADES

El Director General, declara que se hace responsable de la autorización del servicio solicitado por el usuario, de acuerdo al numeral 6.2.5 de la **Directiva Administrativa N.º 229-MINSA/2017/OGTI** "Directiva Administrativa que establece el correcto uso de los servicios informáticos del Ministerio de Salud", publicada en la página Web <https://www.gob.pe/institucion/minsa/normas-legales/190162-119-2017-minsa> comprometiéndose; donde establece que: " El Ministerio de salud, a través de la Oficina de Soporte y Telecomunicaciones, implementará mecanismos o controles de seguridad tales como políticas, equipos informáticos y software corta fuegos o firewall, software antivirus, sistemas de detección y/o prevención de intrusos, filtros de spam, filtros de contenido en internet, sistemas de priorización de paquetes de datos, entre otros, como medidas para prevenir todo riesgo y amenaza que considere que atenten contra un activo de la información. Así mismo, el usuario solicitante declara conocer el numeral 6.2.5 de la Directiva en mención, comprometiéndose al buen uso de los accesos otorgados, así como a no compartir los mismos con otros usuarios no autorizados.

Usuario Solicitante	Director General / Ejecutivo Área Solicitante	Oficial de Seguridad de la Información OGTI	Oficina de Soporte e Infraestructura Tecnológica - OGTI
			

RIESGOS Y RESPONSABILIDADES ASOCIADAS A LOS ACCESOS DE USO DE MEMORIAS USB CONFORME A LA NORMATIVA PERUANA Y LA ISO 27001

Riesgos Asociados al Uso de Memorias USB:

Propagación de malware: El uso de memorias USB puede facilitar la introducción de virus, ransomware y otros tipos de software malicioso en la red del MINSA, afectando la seguridad de la información y vulnerando los controles de seguridad establecidos en la NTP ISO 27001.

Pérdida de datos confidenciales: El uso de dispositivos de almacenamiento extraíble sin cifrado adecuado puede ocasionar la pérdida o robo de información sensible, infringiendo la Ley de Protección de Datos Personales y la NTP ISO 27001, que exige la protección de datos personales y su acceso autorizado.

Acceso no autorizado: El uso de dispositivos USB puede permitir que personas no autorizadas accedan a información crítica, lo que contraviene los principios de integridad y confidencialidad de la NTP ISO 27001.

Responsabilidades del Solicitante:

Cumplimiento de la normativa vigente: El solicitante debe asegurarse de que el uso de los accesos extendidos cumpla con la Ley N° 29733 y las políticas de seguridad de la NTP ISO 27001, y debe utilizar los recursos solo para los fines laborales que le han sido asignados.

Protección de la información confidencial: El usuario es responsable de garantizar la seguridad y confidencialidad de la información manipulada, conforme a los controles de la NTP ISO 27001 y la normativa peruana de protección de datos personales.

Uso responsable de los recursos tecnológicos: El usuario se compromete a no realizar actividades no autorizadas, como acceder a contenido inapropiado o instalar software no autorizado, según lo establece la NTP ISO 27001.

Registro y auditoría: El usuario acepta que las actividades realizadas bajo los accesos otorgados serán monitoreadas y auditadas conforme a las políticas de la NTP ISO 27001 y la normativa del MINSA.

Cualquier incumplimiento de estas responsabilidades conllevará el retiro de los accesos extendidos, ser reportado ante las autoridades correspondientes, así como la posible aplicación de sanciones administrativas, y las responsabilidades legales derivadas del incumplimiento de la Ley N° 29733 y las políticas de seguridad de la NTP ISO 27001.