
 Sunass <i>El regulador del agua potable</i>	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN		OPERACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	
	FORMATO	SOLICITUD DE HABILITACIÓN O DESHABILITACIÓN DE LA VPN	Versión: 001 Fecha de vigencia: 31/12/2025	
	Código: GTI-OTI-FM012		Página 1 de 5	

SOLICITUD DE HABILITACIÓN O DESHABILITACIÓN DE LA VPN

ROL	NOMBRE	CARGO/ROL
Elaborado por:	Janeth Ingebore Cabrera Jauregui	Especialista en Seguridad Informática
Revisado por:	Gustavo Adolfo Bernal Soto	Jefe de la Unidad de Modernización
	Angel Enrique Felix Garcia	Oficial de Seguridad y Confianza Digital
	Renato Adrián Delgado Flores	Jefe de Oficina de Asesoría Jurídica
Aprobado por	Eduardo Martín Morán Huanay	Jefe de la Oficina de Tecnologías de Información

	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN		OPERACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	
	FORMATO	SOLICITUD DE HABILITACIÓN O DESHABILITACIÓN DE LA VPN		Versión: 001 Fecha de vigencia: 31/12/2025
	Código: GTI-OTI-FM012			Página 2 de 5

CONTROL DE CAMBIOS

N°	Ítems	Descripción del cambio
-	-	Versión inicial del documento

1. DATOS DEL USUARIO

(Se registran los datos de la persona cuyo acceso VPN será habilitado o deshabilitado)

Apellidos y Nombres			
Documento de Identidad			
Cargo / Rol (si aplica)			
Unidad de Organización	<Señalar la unidad de organización en la que labora o presta servicios. Ejemplo: Unidad de Contabilidad, Unidad de Abastecimiento, Dirección de Fiscalización, entre otros>		
Sede			
Correo electrónico			
Tipo de vínculo con la Sunass	<input type="checkbox"/> CAS <input type="checkbox"/> CAP <input type="checkbox"/> Locador <input type="checkbox"/> Proveedor (persona jurídica o natural distinta al locador)		
	Solo para usuarios externos (locador/proveedor)		
	N.º Contrato u Orden de Servicio: (adjuntar la copia del documento)		
	RUC y Razón Social: (Completar si el proveedor es persona jurídica)		

2. DATOS DEL RESPONSABLE DE LA UNIDAD ORGANIZACIÓN

Apellidos y Nombres	
Cargo	
Correo institucional	

3. REQUERIMIENTO

3.1 TIPOS DE SOLICITUD

☐ Habilitar acceso VPN

• Horario de conexión requerido

☐ 5x8 (Lunes a Viernes – horario laboral).

☐ 7x24 (Lunes a Domingo – incluye fines de semana)*

*Requiere justificación especial, sustentar en el numeral 3.2.

• Vigencia de acceso (máximo hasta 90 días calendarios)

Desde _____ hasta _____

(Al finalizar la vigencia, el acceso será deshabilitado automáticamente)

Nota:

- El usuario debe firmar el Anexo de este formato.
- Para renovaciones de acceso VPN, se deberá presentar una nueva solicitud antes del vencimiento del periodo vigente.

☐ Deshabilitar acceso VPN

(Solo aplica cuando se requiera la baja anticipada del acceso)

3.2 JUSTIFICACIÓN

Si se trata de una habilitación:

<Explique de forma clara y concisa la necesidad de la habilitación del acceso a la VPN, especificando que funciones requieren acceso remoto, porque es necesario el acceso VPN para estas funciones y cuáles son los riesgos o impacto institucional de no contar con dicho acceso>.

Si se trata de una deshabilitación:

<Explique claramente el motivo de la deshabilitación anticipada, tales como: Finalización anticipada del contrato u orden de servicio, periodos de descanso vacacional o licencias, Incumplimiento de obligaciones contractuales o políticas de seguridad, entre otros>

3.3 AUTORIZACIÓN DE LA UNIDAD DE ORGANIZACIÓN


Autorizo la presente solicitud para el usuario solicitante, en función de las necesidades de la **<colocar la unidad de organización>** indicadas en este documento.

(marque según el tipo de solicitud seleccionado en la sección 3.1 de este formato)

- ☐ Confirmando que la necesidad **del acceso por VPN** está debidamente justificado para el cumplimiento de funciones institucionales o contractuales vinculadas a la Sunass; asimismo el usuario autorizado es responsable del cumplimiento de todas las medidas de seguridad que se aplican para el uso del mencionado acceso, conforme a lo detallado en los "Lineamientos Específicos de Seguridad de la Información"¹ vigentes y de aplicación obligatoria en toda la institución y lo establecido en el Anexo de este documento que el usuario debe firmar.
- ☐ Confirmando que el motivo de la **deshabilitación del acceso VPN** está debidamente justificado en la sección 3.2 y que se ha verificado el cumplimiento o conclusión de las obligaciones contractuales/laborales que justificaban el acceso.

Firma del/de la responsable de la Unidad Organización

¹ Aprobados en la directiva GDI-MAS-DI001 "Lineamientos Específicos de Seguridad de la Información" publicada en el Portal del SIG.

 El regulador del agua potable	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN		OPERACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
	FORMATO	SOLICITUD DE HABILITACIÓN O DESHABILITACIÓN DE LA VPN	Versión: 001 Fecha de vigencia: 31/12/2025
	Código: GTI-OTI-FM012		Página 5 de 5

ANEXO

DECLARACIÓN DEL USUARIO DE LA VPN

Declaración

Al presentarse la solicitud, me comprometo a cumplir con los siguientes compromisos y condiciones establecidas a continuación en el marco de mi vínculo laboral o contractual con la Sunass:

Compromisos de Uso

1. Utilizar el acceso a la VPN exclusivamente para el desarrollo de funciones institucionales o actividades contractuales autorizadas, quedando prohibido su uso para fines personales o no autorizados.
2. Mantener bajo absoluta confidencialidad las credenciales de acceso a la VPN, sin compartirlas ni permitir su uso a personas no autorizadas.
3. Permitir el acceso remoto o presencial al personal de la Oficina de Tecnologías de la Información (OTI), a fin de garantizar la actualización de antivirus y demás controles de seguridad, siempre que se trata de equipos de la Sunass.
4. Cuando se usen equipos propios (locadores, proveedores, CAS o CAP), garantizar que cuenten con antivirus y sistema operativo actualizado y medidas de seguridad exigidas en el contrato o lineamientos específicos de seguridad de la información de la Sunass.
5. Cumplir los lineamientos específicos de seguridad de la información establecidos por la Sunass y las disposiciones técnicas establecidas por la OTI.
6. Reportar de manera inmediata, a través del Sistema de Mesa de Servicios (<https://mesadeservicio.sunass.gob.pe/asmscustomer/index.html#/>) cualquier evento o incidente de seguridad que se presente durante el uso de la VPN (por ejemplo, accesos no autorizados, pérdida o compromiso de credenciales), para conocimiento y atención del Oficial de Seguridad y Confianza Digital.

Reconocimiento de riesgos

Reconozco y acepto que:

1. El uso de la VPN conlleva riesgos tales como:
 - Accesos indebidos sino protejo mis credenciales.
 - Pérdida de confidencialidad de la información institucional.
 - Exposición a amenazas externas si no cumplo las medidas de seguridad.
2. Las conexiones realizadas a través de la VPN, así como el uso de los recursos institucionales, pueden ser monitoreados y registrados por la OTI con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de la Sunass.
3. Soy el único responsable del uso que haga del acceso VPN otorgado.

Aceptación

Declaro haber leído y comprendido los compromisos y condiciones establecidas en este documento, y acepto cumplirlos íntegramente. Asimismo, comprendo que el incumplimiento dará lugar a la revocación inmediata del acceso, y según corresponda, a medidas administrativas, contractuales o legales que resulten aplicables.

Firma del/de la usuario/a