PONTIFICIA UNIVERSIDAD CATOLICA DE VALPARAISO

PUCV Calidad de Servicio

VICERRECTORÍA DE ADMINISTRACIÓN Y FINANZAS

[Políticas de Uso]

DSIC

Dirección de Servicios de Informática y Comunicaciones

[I] ÍNDICE

[I] ÍNDICE

LISTA DE TABLAS

[1] CONTEXTO GENERAL

[1.1] ÁMBITO DEL SERVICIO

Las normas mencionadas en este apartado, propician el uso apropiado del sistema de Red Privada Virtual, y aplica a todos los miembros de la comunidad universitaria para quién fue definido el servicio, ya sean estos docentes, alumnos o funcionarios y en general cualquier usuario que haga uso de forma autorizada.

La Universidad sólo proveerá la habilitación del usuario dentro del sistema VPN implementado en la DSIC, el cual no tiene costo alguno para el usuario.

Ante lo cual cualquier costo que el usuario genere para hacer uso de este servicio, será de su exclusiva responsabilidad. Estos costos se pueden originar producto de la contratación de un servicio de Internet o bien del soporte para instalación de software necesario.

[1.2] DISPONIBILIDAD DEL SERVICIO

El servicio de VPN-PUCV estará disponible las 24 horas del día, todos los días de la semana.

[2] NORMAS DE USO VPN

[2.1] ALCANCE CONEXIÓN VPN PUCV

1. Para garantizar el buen uso de la tecnología VPN, los usuarios declaran conocer que sus equipos, ya sea institucionales o personales forman parte de una extensión de la red de la Universidad, por lo tanto están sujetos a las mismas normas y reglamentos que se aplican a los equipos dentro de las dependencias de la PUCV.

2. Sólo usuarios previamente autorizados podrán utilizar los beneficios del Sistema VPN, los que además, serán los responsables del correcto uso del servicio de acceso remoto.

3. Las cuentas VPN-PUCV son exclusivamente de uso personal y exclusivo, para quienes se les ha asignado dichos privilegios, por lo cual está estrictamente prohibido facilitar el acceso a terceras personas.

[2.2] ACCESO A LAN PUCV

1. El servicio VPN otorgará al usuario acceso seguro a la red LAN de la PUCV.

2. El acceso de usuarios a la red LAN de la universidad a través de una conexión VPN, debe ser realizado única y exclusivamente utilizando el puerto habilitado para dicho fin.

3. El puerto de acceso a la red LAN de la universidad, debe ser habilitado por el administrador del servicio.

4. Cada usuario solo podrá tener activa una solo conexión VPN-PUCV.

5. Una vez que hayan transcurrido 10 minutos de inactividad, los usuarios del sistema VPN serán automáticamente desconectados de la sesión. El usuario deberá logearse nuevamente para volver a conectarse a la red universitaria.

[2.3.3] CAMBIO DE CLAVE

Para solicitar un cambio de clave, el usuario debe comunicarse con el Área de Soporte de la DSIC vía teléfono o bien a través de la dirección de correo: soporte.dsic@ucv.cl.

[2.4] ELIMINACIÓN DE CUENTAS VPN

[2.4.1] ELIMINACIÓN POR SOLICITUD

Si el usuario por alguna razón desea eliminar su cuenta VPN-PUCV, debe solicitar dicho procedimiento a través de un correo electrónico a la dirección: soporte.dsic@ucv.cl.

[2.4.2] ELIMINACIÓN POR INACTIVIDAD

1. Si el usuario no ha utilizado su cuenta de acceso VPN-PUCV en un periodo de tiempo de 11 meses consecutivos, la DSIC le informará vía correo electrónico que su cuenta queda suspendida por tal motivo.

2. Si el usuario no responde al aviso realizado en el onceavo mes, al cumplirse el año de inactividad, inmediatamente la cuenta queda eliminada del sistema.

3. Si el usuario desea tener nuevamente una cuenta VPN-PUCV, deberá volver a realizar la solicitud.

[2.4.3] ELIMINACIÓN POR DESVINCULACIÓN DE LA INSTITUCIÓN

Si el usuario ha sido desvinculado de la institución, su cuenta de acceso VPN-PUCV será caducada.

[2.2.1] ACCESO SEGURO AL COMPUTADOR PUCV

1. Si el usuario desea acceder a su computador de la PUCV desde la red WAN en forma segura, éste deberá utilizar el software de acceso remoto recomendado en manual de usuario (Escritorio remoto Windows).

2. Es necesario configurar previamente el servicio de escritorio remoto en el computador al cual se desea acceder, debido a que el servicio VPN por sí solo no habilita dicho acceso.

[2.2.2] ACCESO SEGURO A SERVICIOS PUCV Y TERCEROS

1. A través del servicio de VPN se puede acceder a todos los servicios internos brindados a través de la red de datos de la PUCV.

2. La dirección IP que el servicio de VPN asigna a los usuarios, permite acceder a los recursos y distintos servicios externos a la universidad con los cuales se tiene convenio, tal como bibliotecas de universidades extranjeras – por ejemplo.

[2.3] CLAVES VPN

[2.3.1] ASIGNACIÓN DE CLAVE

Para garantizar el uso personalizado del sistema VPN, se asigna una contraseña de autenticación, la cual nunca deberá ser divulgada, siempre debe ser mantenida en secreto.

[2.3.2] PÉRDIDA DE CLAVE

Si el usuario olvida la clave de su cuenta VPN-PUCV, debe enviar un correo a soporte.dsic@ucv.cl informado de la situación, ante lo cual se generará una nueva contraseña.

[2.5] SITUACIONES ESPECIALES

[2.5.1] PÉRDIDA DE EQUIPO

En el caso que un usuario sufra el robo de su equipo personal debe informar cuanto antes a la DSIC para que la cuenta VPN asignada sea bloqueada. Luego de esto, si el usuario lo solicita se generará una nueva cuenta.

[2.5.2] INGRESO NO AUTORIZADO POR UN TERCERO

En el caso que un usuario detecte que una persona no autorizada haya utilizado su cuenta VPN-PUCV, debe dar aviso cuanto antes a la DSIC, para analizar los pasos a seguir según cada caso particular.

[2.6] VULNERACIÓN DE POLÍTICAS

Los clientes que sean sorprendidos vulnerando o intentado vulnerar las políticas impuestas por la DSIC PUCV, se les bloqueará inmediatamente el acceso al servicio.

[3] SOPORTE

Ante cualquier problema que presente el uso del sistema, se debe informar al personal del Área de Soporte de la DSIC, quienes se encargarán de buscar una solución a dicho problema.

[3.1] HORARIOS DE ATENCIÓN SOPORTE

1. La atención de consultas junto con las distintas actividades de mesa de ayuda relativa al sistema, se realizarán en los siguientes horarios:

Días	Horario de Atención
Lunes a Jueves	8:30 a 18:00
Viernes	8:30 a 17:00
Sábado	9:00 a 13:00

Tabla 1 *Horario de Atención Área Soporte*

2. Una vez recibida la solicitud los tiempos de respuesta máximos de atención definidos son de 24 horas.

[3.2] ÁMBITO DE ATENCIÓN

El soporte computacional para el servicio VPN solo será brindado exclusivamente a personas pertenecientes a la Universidad y no a personas ajenas a ella o a terceros.

[4] BUENAS PRÁCTICAS

[4.1] SEGURIDAD DE ENTORNO

Para evitar errores involuntarios o bien cometidos intencionalmente por terceras personas que por descuido puedan ocupar la conexión VPN asignada, los cuales pueden ser nefatos tanto para el usuario como para la universidad, es necesario tener en cuenta lo valioso que puede ser el hecho de realizar las siguientes actividades:

1. Es importante tener en cuenta que la contraseña de autenticación asignada nunca deberá ser divulgada a terceros, y siempre debe ser mantenida en secreto, lo cual garantiza el uso personalizado y correcto del sistema VPN, y a su vez reguarda el uso de información personal.

2. Configurar el protector de pantalla y la contraseña de entrada del equipo donde instalará la VPN de forma que si deja libre por un momento su estación de trabajo, otra persona no tendrá acceso a los recursos de la PUCV.

3. Desconectar la VPN una vez concluida las operaciones a realizar en la red de la PUCV.

[4.2] RESGUARDO DE LA INFORMACIÓN

1. Un usuario al momento de ingresar al dominio de la Universidad a través de Internet, debe tener la claridad que desde ese momento se podrá conectar a todos los recursos disponibles en la LAN de la PUCV, o bien para decirlo de manera más específica, también el usuario podrá conectarse a un computador residente en las oficinas de la universidad. Por lo tanto todos los recursos alcanzables por una conexión VPN, como son Bases de Datos personales, Bases de Datos corporativas, correos electrónicos, documentos residentes en carpetas compartidas o bien en unidades remotas, se pueden ver afectados por un descuido o mal uso.

2. Se recomienda tomar los resguardos necesarios conducentes a conservar la integridad de la información a la cual se tenga acceso, para eso se deben tomar las debidas precauciones de conexión y desconexión recomendadas por esta DSIC.

3. Independiente del buen uso que se le dé al servicio VPN, es conveniente realizar respaldos periódicos de toda la información que está bajo su responsabilidad, como pueden ser bases de datos, informes, etc.

4. Esta aplicación solo debe ser instalada en equipos que estén bajo responsabilidad de personas que tengan algún tipo de vínculo contractual con la universidad, por consiguiente, esta DSIC validará el estatus PUCV de la persona solicitante.

5. Esta aplicación no debe ser instalada en Cibercafés ni en equipos de uso público.

DSIC / Dirección de Servicios de Informática y Comunicaciones
Contacto 227 3050 / **Correo Electrónico** dsic@ucv.cl
Call Center Central 227 3400
Call Center Curauma 227 4600 / **Correo Electrónico** soporte@ucv.cl

Pontificia Universidad Católica de Valparaíso / Dirección General de Asuntos Económicos y Administrativos / Av. Brasil 2950 Valparaíso.Chile