

Términos y Condiciones de Uso del Servicio de VPN

Fecha de emisión o actualización: 07/03/2022

Código: CI-AGS-T04

Versión: 2.1

Lineamiento CI-1-2022

TABLA DE CONTENIDOS

1. INTRODUCCIÓN	3
2. DEFINICIONES Y ABREVIATURAS	3
3. DESCRIPCIÓN DEL SERVICIO	4
4. REFERENCIA LEGAL O NORMATIVA.....	4
5. CARACTERÍSTICAS O CONDICIONES DEL SERVICIO	5
6. COMPROMISOS CON EL USUARIO	8
7. MÉTRICAS DEL SERVICIO	8
8. COMPROMISOS DEL USUARIO	9
9. DOCUMENTACIÓN TÉCNICA DE REFERENCIA	10
10. CONTACTO PARA SOPORTE TÉCNICO Y ADMINISTRACIÓN DEL SERVICIO	11
11. APROBACIÓN.....	11
12. ANEXOS	11

1. INTRODUCCIÓN

El servicio de acceso remoto por VPN es un servicio que la Universidad de Costa Rica ofrece para tener

acceso a información y equipos de TI en la RedUcr, desde un sitio remoto a través de Internet. Por tal razón, el Centro de Informática define las siguientes regulaciones y condiciones para su uso.

2. DEFINICIONES Y ABREVIATURAS

- ⑩ **Acceso VPN punto a punto:** conexiones virtuales entre servidores institucionales y servidores de terceros que pueden ser nacionales o internacionales (bancos, universidades, centros de investigación, entre otros).
- ⑩ **CI:** Centro de Informática.
- ⑩ **DTSE:** Directrices Técnicas de Seguridad de la Información.
- ⑩ **Local Area Network (LAN):** Red de área local.
- ⑩ **RedUcr:** es la red de la Universidad de Costa Rica.
- ⑩ **GIT:** Gestor de Tecnologías de Información.
- ⑩ **UCR:** Universidad de Costa Rica.
- ⑩ **Usuario:** quien hace uso del servicio provisto, según la aprobación de la jefatura correspondiente.
- ⑩ **VPN (Virtual Private Network):** tecnología de red de computadoras que permite una extensión segura de la red interna de la Universidad sobre una red pública o no controlada como Internet.

3. DESCRIPCIÓN DEL SERVICIO

El servicio VPN (Virtual Private Network), brindado por el CI tiene dos modalidades: una permite a los usuarios de la Universidad de Costa Rica conectarse desde Internet a dispositivos restringidos de la RedUCR y la otra permite la interconexión de servicios de TI entre instituciones.

Este servicio a su vez, admite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de

la RedUcr.

4. REFERENCIA LEGAL O NORMATIVA

- ⑩ El “Reglamento General de las Oficinas Administrativas”, de la Universidad de Costa Rica, en su Capítulo III, Artículo 9 inciso “f” y en el Artículo 10, inciso “o”, indica:

“f) Emitir directrices, supervisar y establecer procedimientos de acatamiento obligatorio, propias de su área de competencia”.

“o) Establecer, en conjunto con el Consejo Técnico Asesor, las directrices propias del quehacer y prioridad de la oficina a su cargo”.

- ⑩ El reglamento vigente del Centro de Informática establece en el Artículo 2:

punto 3. Emitir lineamientos, directrices, estándares y normas, acorde con el área de competencia, según lo que establece el Reglamento de Oficinas Administrativas.

punto 4. Definir, desarrollar y proponer a la Administración Superior y a la comunidad universitaria las directrices, lineamientos, planes, estándares y normas para la adquisición de productos y servicios de tecnologías de información y comunicación.

- ⑩ Directrices de Seguridad de Información de la Universidad de Costa Rica (R-102-2015)”, Capítulo 13 Control de accesos, Artículos 44 y 45, donde se determina lo siguiente:

Artículo 44: Se establecen los controles para el acceso a la información, a los sistemas y a los procesos institucionales, mismos, que deberán ser consistentes con los requerimientos de seguridad propios de la información de que se trate y de los objetivos que se haya trazado la Universidad, contemplados en las DTSI, así como en los estándares, lineamientos y procedimientos formalmente aprobados”.

ARTÍCULO 45. Requerimientos corporativos del control de accesos: La Universidad de Costa Rica controlará el acceso a la información, a los servicios, sistemas y a los procesos institucionales de acuerdo a las Directrices que para ese fin se establecen, así como, en los estándares y procedimientos formalmente aprobados.

5. CARACTERÍSTICAS O CONDICIONES DEL SERVICIO

Para optar por el “servicio VPN” es necesario que el jefe o director¹ de la unidad interesada, envíe la solicitud al Director de la Unidad del Centro de Informática.

Para ello se debe ingresar en el sitio WEB del CI (<http://ci.ucr.ac.cr>) y completar el formulario que corresponda² de acuerdo con el servicio requerido, adjuntar la documentación que respalde dicha solicitud y remitirla por medio del sistema de reportes de solicitudes y averías del Centro de Informática. Una vez que el funcionario asignado del CI realice el estudio respectivo, el resultado se hará llegar a la unidad usuaria en un plazo no mayor a 10 días hábiles al contacto indicado en el formulario.

Previo a solicitar el servicio considere lo siguiente:

- ⑩ La vigencia del servicio tiene como plazo máximo 1 año a partir de la fecha de aprobación de la solicitud.
- ⑩ La solicitud que se justifica con una figura de “teletrabajo” debe venir acompañada de documentación de respaldo de la Oficina de Recursos Humanos o de la Vicerrectoría de Administración.
- ⑩ La solicitud que se justifica con una figura de “trabajo remoto”, debe venir acompañada de la autorización del jefe de la Unidad, en la que labora el usuario o usuaria a para el cual se solicita el servicio de VPN.
- ⑩ El solicitante debe disponer de un usuario en el directorio institucional, para que se le asigne el rol de VPN. En caso que no lo tenga el CI lo facilitará una vez que se haya aprobado la solicitud.
- ⑩ En los casos donde se solicita el servicio para un tercero que es contratado para brindar servicios de soporte, vigilancia y desarrollo, la responsabilidad del uso del servicio aprobado recae sobre la Unidad a cargo de la contratación.
- ⑩ El acceso a servicios y plataformas que se accederán a través de la VPN, deben ser tramitados

¹Lista dispuesta por el Consejo Universitario en la sesión N.º 4031, artículo 8, del 11 de mayo de 1994, <http://www.cu.ucr.ac.cr/autorid.php>

²CI-AGS-F43 Solicitud del servicio de VPN para usuarios

 UNIVERSIDAD DE COSTA RICA	TÉRMINOS Y CONDICIONES DE USO DEL SERVICIO DE VPN			
	Código: CI-AGS-T04	Versión: 2.1	Página 6 de 10	

previamente ante sus respectivos encargados.

5.1 PERFILES DE ACCESO DEL SERVICIO

- ⑩ En caso de ser requerido, el CI puede modificar el perfil existente en lo referente a las redes IP de la UCR que puede alcanzar mediante la conexión VPN y añadir otros perfiles de usuarios que se ajusten a nuevas necesidades.
- ⑩ Todos los usuarios en un mismo perfil, tienen acceso a los mismos segmentos de direcciones IP de la RedUCR.

5.2 HORARIO Y ATENCIÓN

- ⑩ El servicio funciona todos los días del año durante las 24 horas del día.
- ⑩ El soporte que brinda el Centro de Informática para el servicio de VPN es en el horario de lunes a viernes de 8:00 a.m. a 12:00 medio día y de 1:00 p.m. a 5:00 p.m.
- ⑩ La atención de incidentes sobre el servicio de VPN, no se brinda en los periodos especiales de cierre de las instalaciones de la Universidad por receso, feriados o días de asueto.
- ⑩ El plazo que dispone el CI para atender los incidentes reportados, es de 2 horas como máximo, siempre en horario hábil. Para los incidentes que no pueden ser resueltos en el plazo descrito, el Centro notificará al usuario o a la Comunidad Universitaria, las explicaciones correspondientes que justifiquen la no atención en el plazo acordado.

5.3 SOPORTE TÉCNICO

El servicio técnico que brinda el CI es en la plataforma que sustenta el servicio de VPN, como por ejemplo equipos de la RedUCR y de autenticación, además proporciona a los usuarios la guía técnica³

³http://apuntes.ucr.ac.cr/index.php/Configura%C3%B3n_de_cliente_de_correo_con_cuenta_institucional_de_correo_electr%C3%B3nico

para utilizar el servicio. Se excluye de las labores de este soporte, la configuración de la conexión - VPN en el dispositivo del usuario, cualquier problema asociado a ello y a la conexión de internet del dispositivo.

5.4 MANTENIMIENTO CORRECTIVO Y PREVENTIVO

El CI realiza al año al menos una actividad de mantenimiento preventivo en el servicio de VPN, la cual se notificará a la Comunidad Universitaria con 8 días naturales de anticipación.

En caso de que se deban realizar tareas de mantenimiento correctivo al servicio VPN por imprevistos y es necesario suspender dicho servicio, se notificará a la Comunidad Universitaria tan pronto como sea posible, para que se tomen las consideraciones correspondientes.

6. COMPROMISOS CON EL USUARIO

Garantizar el servicio de VPN al usuario durante el tiempo en que se le haya aprobado el uso de este servicio, para ser utilizado en las actividades propias de sus funciones de la Institución.

Esas actividades son de uso exclusivo de los recursos existentes en la red interna de la RedUCR.

7. MÉTRICAS DEL SERVICIO

Como métrica del servicio se considera el nivel de disponibilidad, el cual se estima en un 99,8%. Esta medición se obtiene de la plataforma de monitoreo que para tal fin tiene el CI.

Se considera falta de disponibilidad del servicio de VPN cuando se verifique la suspensión de dicho servicio por problemas directamente imputables a los equipos de la RedUCR, se excluyen causas como mantenimientos programados, fallos eléctricos, problemas en el servicio de Internet ofrecido por los proveedores. El nivel de disponibilidad es calculado en función a la siguiente tabla:

Caídas de más de 5 minutos y menos de 9 horas semestrales	Disponibilidad de 99.8% al 99.99%
Caídas de más de 9 horas y menos de 67,5 semestrales	Disponibilidad del 99% al 99.8%
Caídas de más de 67, 5 horas semestrales	Disponibilidad de menos del 99%

8. COMPROMISOS DEL USUARIO

El usuario del servicio VPN de la Universidad de Costa Rica se compromete a aceptar y cumplir los siguientes términos y condiciones:

- ⑩ Utilizar el servicio sólo para fines propios de las actividades académicas, acción social, investigación y administrativas de la Universidad, buscando proteger la reputación y el buen nombre de la Universidad mediante un uso adecuado del mismo.
- ⑩ Debe utilizar eficientemente la RedUCR, con el fin de evitar en la medida de lo posible la congestión de la misma.
- ⑩ Utilizar la conexión de acceso remoto solo para acceder a servicios exclusivos de la Universidad los cuales sean inalcanzables desde Internet.
- ⑩ El servicio de VPN no se debe utilizar desde computadores no confiables como cafés Internet, aeropuertos, hoteles, entre otros.
- ⑩ Abstenerse de usar el servicio VPN en caso de que el dispositivo que inicia la conexión esté infectado por virus, ransomware, malware o cualquier otra amenaza informática.
- ⑩ Desconectarse del servicio una vez finalizada la sesión de tareas o consultas a realizar o cuando necesite retirarse del computador momentáneamente.
- ⑩ Las credenciales de acceso no se deben compartir, excepto en los casos explícitamente en que el servicio se otorgó para que la Unidad pueda recibir soporte o asistencia de un externo.
- ⑩ Cuando se sospeche que la cuenta haya sido vulnerada o presente un problema de seguridad, se debe de comunicar inmediatamente al Centro de Informática.
- ⑩ El servicio de VPN no debe utilizarse para actividades informáticas tales como escaneo de equipos, escaneo de vulnerabilidades, ataques de cualquier índole, pruebas de rendimiento que puedan desestabilizar la RedUCR y los equipos conectados a ella.

- ⑩ Cumplir con las políticas de uso de los sistemas e información de su oficina o dependencia, considerando aspectos de horario, procesos en los que interviene y funciones asignadas.
- ⑩ Cuando se solicita el servicio de VPN, la persona usuaria se da por enterada y acepta que ha leído y entendido estas condiciones y términos que el Centro de Informática ha establecido para su uso. Cuando la persona usuaria incumpla alguno de los términos y condiciones del servicio, el CI puede suspender el servicio y notificar al siguiente día hábil.

He leído y entendido estos términos y condiciones de uso de VPN establecido por el Centro de Informática. Estoy de acuerdo en acatar las directrices anteriores y entender que el incumplimiento de estas, pueden resultar en el bloqueo de mis derechos para su uso y asumir las sanciones legales si corresponde.

9. DOCUMENTACIÓN TÉCNICA DE REFERENCIA

A continuación se detalla la normativa, la documentación, técnica y de tramitología publicada en el sitio web del Centro de Informática (ci.ucr.ac.cr), asociada a estos términos y condiciones.

- ⑩ Directrices de Seguridad de la Información de la Universidad de Costa Rica (https://ci.ucr.ac.cr/sites/default/files/informaciondigital/Resolucion_R-102-2015.pdf)
- ⑩ CI-AGS-F43 Solicitud del servicio de VPN para usuarios.

10. CONTACTO PARA SOPORTE TÉCNICO Y ADMINISTRACIÓN DEL SERVICIO

Cada usuario puede notificar cualquier incidente o problema, por medio del sistema de reportes de solicitudes y averías ubicado en el sitio <http://ci.ucr.ac.cr> o a la extensión 5000 del Centro de Informática (Atención de Usuarios).

Adicionalmente se dispone del correo ci5000@ucr.ac.cr como un buzón exclusivo para consultas rápidas

11. APROBACIÓN

Actividad	Responsable
-----------	-------------

 UNIVERSIDAD DE COSTA RICA	TÉRMINOS Y CONDICIONES DE USO DEL SERVICIO DE VPN			
	Código: CI-AGS-T04	Versión: 2.1	Página 10 de 10	

Actualización	Heylin Pacheco
Revisión UCM	Heylin Pacheco
Aprobación coordinación	Wilfredo Fonseca
Aprobación Dirección	Henry Lizano

<Firma marca de agua>

12. ANEXOS

No aplica.