1. PROPÓSITO

Establecer los lineamientos de seguridad de la información que deben ser acatados por las personas trabajadoras de la Universidad que realizan actividades teletrabajables y hacen uso de los equipos, recursos, bases de datos y servicios de tecnología de la Institución.

2. TÉRMINOS Y ABREVIATURAS

- **Actividad teletrabajable:** conjunto de tareas que la organización determina que pueden ser realizadas fuera de las instalaciones de los centros habituales de trabajo, utilizando medios telemáticos para el desarrollo normal de la actividad laboral, sin afectar el desempeño de la misma y el servicio al usuario.
- **CI:** Centro de Informática.
- **DTSI:** Directrices Técnicas de Seguridad de la Información.
- **VPN:** Red Privada Virtual.
- **Herramientas colaborativas:** Aplicaciones de videollamadas, correo electrónico, acceso a la red privada, herramientas de ofimática autorizadas y aquellas que la Administración vaya indicando mediante resoluciones adicionales.

3. LEYES, REGLAMENTOS O DOCUMENTOS DE REFERENCIA

- 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 que le corresponde al Centro de Informática:
  “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”

- 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.

- Las Directrices Técnicas de Seguridad de Información de la Universidad de

Costa Rica (DTSI) R-102-2015), en el *"capítulo 8 Resguardo y protección de la información", los artículos 18 y 21* estipulan lo siguiente:

- *Artículo 18: La protección de la información por parte del personal usuario, como un elemento fundamental en la cadena de aseguramiento de ésta, aborda la necesidad de considerar al recurso humano como elemento prioritario en la protección de la información, estableciendo controles referentes a la propiedad de la información, la elaboración de respaldos, y la protección de registros.*
- *Artículo 21: Respaldos y recuperación de la Información: La información que la Universidad de Costa Rica determine como esencial deberá ser respaldada y resguardada en instalaciones seguras y controladas, a fin de que la misma pueda recuperarse una vez ocurrido un desastre, siniestro, emergencia o falla en/de los dispositivos y/o sistemas. Los Jerarcas y Titulares Subordinados deberán velar porque existan procedimientos y controles en sus áreas y unidades, que permitan recuperar la información y que dichos procedimientos y controles sean periódicamente evaluados, para asegurar una continuidad de las operaciones en productos y servicios.*

⑩ Reglamento para la administración y control de los bienes institucionales de la Universidad de Costa Rica.

4. LINEAMIENTOS

4.1 Las personas trabajadoras que realicen actividades teletrabajables, deben utilizar las herramientas colaborativas dispuestas por la Universidad.

4.2 Cuando se requiera de una conexión remota a la RedUCR a través de una VPN, para ejecutar las actividades teletrabajables, el responsable de la Unidad de trabajo podrá solicitarlo a través de en la página del Centro de Informática en el sistema de "solicitudes y averías" o por oficio, siguiendo el proceso establecido. Será el encargado del Centro de Informática asignado para esa solicitud, quien valorará el requerimiento y facilitará el acceso correspondiente.

4.3 El equipo en el cual se instalará la VPN debe ser preferiblemente una computadora propiedad de la Universidad de Costa Rica, que tenga instalada la última versión del antivirus institucional. En casos excepcionales, si esto no es posible, la persona funcionaria se compromete a que el equipo personal donde se instalará el VPN, cuente con el sistema

operativo y antivirus actualizados, lo anterior con el fin de disminuir los riesgos de seguridad para la plataforma de la UCR.

4.4 La persona trabajadora que cuente con una VPN para llevar a cabo las actividades teletrabajables, debe cumplir lo siguiente:

- Evitar el establecimiento de conexiones a redes inalámbricas desconocidas o que estén habilitadas sin seguridad, es decir, que no solicite claves de ingreso.
- Las credenciales asignadas para el establecimiento de la VPN son de uso personal e intransferible, por tanto, no deben compartirse o divulgarse. El uso inadecuado de las mismas es responsabilidad del propietario.
- Utilizar el VPN únicamente para aspectos laborales y exclusivamente por la persona trabajadora de la UCR a la que le fue asignado el servicio.

4.5 En caso de requerir almacenamiento de información en discos locales de un equipo asignado por la Institución, se debe habilitar el uso de contraseña segura para acceso al equipo y realizar un respaldo periódico de la información en los repositorios institucionales, para prevenir que ante una situación de hurto del equipo de cómputo, se pierda y exponga la información de la institución.

4.6 En caso de requerir documentos físicos o información en dispositivos de almacenamiento extraíbles (como USB Drive, CD, discos duros externos, entre otros) para la ejecución de las actividades teletrabajables, la persona trabajadora es responsable por la custodia y preservación de los mismos; se recomienda no dejarlos expuestos a terceros no autorizados, guardarlos bajo llave y en un lugar seguro.

4.7 Cuando las actividades teletrabajables lo requieran y la jefatura brinde el visto bueno, se podrá facilitar una extensión telefónica por software, que se conecta y registra con los servidores de telefonía de la Universidad, por medio de la VPN que se tenga disponible. Lo anterior acorde a la capacidad de infraestructura con que cuente la plataforma de telecomunicaciones de la Universidad. El uso de esta telefonía se limita al uso de las actividades laborales únicamente.

4.8 Se debe evitar el intercambio de información institucional sensible mediante la comunicación telefónica con personas ajenas a la Universidad, puesto que esta herramienta facilita la aplicación de técnicas de ingeniería social que podrían afectar a la Universidad y a la persona que realiza las actividades teletrabajables, por ejemplo, mediante estafas telefónicas.

4.9 En relación al acceso a servidores de archivos asignados a las Unidades y administrados por los Administradores de Recursos Informáticos Desconcentrados (RID) para actividades teletrabajables, deben:

- Velar por la seguridad y confidencialidad de la información contenida en los servidores de archivo.
- Evitar compartir el acceso al equipo de cómputo con personas no autorizadas, para reducir el riesgo de uso no permitido o ilegal de la información y sistemas de información de la Universidad.

4.10 El acceso a los sistemas de información para actividades teletrabajables, se otorga de acuerdo con los perfiles establecidos, según las labores propias del cargo. La persona trabajadora, por lo tanto, tiene que:

- Acceder con las credenciales personales asignadas a los sistemas de información.
- Las credenciales asignadas para el acceso a los sistemas de información, son de uso personal e intransferible, por tanto, no deben compartirse o o divulgarse.
- Salvaguardar la información contenida en los diferentes sistemas de información a los que se tenga acceso autorizado, evitando compartir el acceso con personas ajenas a la institución.

4.11 En el caso del hardware y software otorgado por la Universidad para el desarrollo de actividades teletrabajables, se debe utilizar únicamente para llevar a cabo las actividades laborales asignadas por la Universidad. Por lo anterior se debe cumplir lo siguiente:

- Evitar abrir correos electrónicos, descargar o ejecutar archivos de los cuales no se conozca su procedencia.
- Evitar abrir y ejecutar ventanas emergentes, barras de herramientas, programas, enlaces desconocidos; estos pueden conducir a sitios de suplantación web para capturar datos que pueden afectar la disponibilidad, integridad y confidencialidad de la información de la Universidad.
- Evitar instalar programas ajenos a los autorizados por la Universidad o que no correspondan al desarrollo normal de las actividades asignadas.
- Comprobar el correcto funcionamiento de la herramienta de antivirus instalada para proteger el equipo de amenazas de virus y, en caso que se presente alguna falla reportar por medio del sistema de “solicitudes y averías”, que el CI tiene disponible en su sitio Web.

4.12 La persona trabajadora es responsable por los daños ocasionados al equipo de cómputo asignado por la Universidad, generado por mal uso del mismo en el desarrollo de actividades teletrabajables, por lo tanto tiene que:

- Cumplir con lo establecido en el *Reglamento para la administración y control de los bienes institucionales de la Universidad de Costa Rica*.
- Evitar exponer el equipo de cómputo en zonas donde exista alta humedad.
- Evitar que el equipo sea golpeado y no consumir líquidos o alimentos cerca del equipo mientras se desarrollan las actividades teletrabajables.
- Evitar utilizar o dejar el equipo de cómputo donde pueda sufrir calentamiento excesivo.
- No hacer ningún tipo de modificación en el hardware que no esté autorizada.

4.13 Respetar y aplicar toda la normativa establecida por parte de la Universidad referente a Seguridad de la Información.

Estos lineamientos para la seguridad informática de actividades teletrabajables, son de acatamiento obligatorio a partir de 06 de julio 2020.

5. APROBACIÓN

Actividad	Responsable	Firma
Elaboración	Marielos Sánchez Velazco (URS)	
Revisión	Ana Cecilia Vargas (URS) Edgardo Baltodano (AGU) Juan José León (AGS) Jorge Alvarado Zamora (ADS) Luis Jiménez Cordero. Sub-Director	
Aprobación	Alonso Castro Mattei. Director	