1. PROPÓSITO

Establecer los requerimientos y pautas que deben cumplir los usuarios cuando establecen conexiones de acceso remoto a recursos, sistemas y aplicaciones institucionales desde fuera de la RedUCR y aplica para la comunidad universitaria.

2. TÉRMINOS Y ABREVIATURAS

2.1 **Acceso Remoto:** Se refiere a la tecnología que permite al usuario remoto acceder a un servidor, plataforma o servicio desde dispositivos que no se encuentran conectados en el entorno de RedUCR, incluye: SSH, RDP y similares.

2.2 **Autenticación multifactor (MFA):** Un proceso de seguridad que requiere que los usuarios proporcionen dos o más formas de identificación para acceder a un sistema.

2.3 **BYOD** (Bring your own device, en inglés): "Trae tu propio dispositivo", se refiere a una práctica que permite a los miembros de la comunidad universitaria el uso apropiado de sus propios dispositivos personales para acceder a los recursos de la UCR.

2.4 **CI**: Centro de Informática.

2.5 **Contraseña segura**: Una contraseña segura es una combinación de letras mayúsculas y minúsculas, números y símbolos especiales (tales como: !@#$%^&*) de doce (12) o más caracteres. No se debe usar la misma contraseña para diferentes servicios.

2.6 **Equipo remoto**: Dispositivo electrónico propio o ajeno a la UCR que es utilizado establecer un acceso remoto.

2.7 **MS Teams**: Plataforma unificada de comunicaciones y colaboración de Microsoft.

2.8 Protocolo de escritorio remoto (RDP): Un protocolo que permite a los usuarios controlar una computadora de forma remota.

2.9 **Lista blanca** (Whitelist) de software: Lista donde se establece qué aplicaciones y software en general pueden acceder determinados sistemas y servicios en la RedUCR.

2.10 **Recursos informáticos:** Lo conforman los componentes, dispositivos o herramientas que se utilizan en el campo de la informática y la tecnología para procesar, almacenar, transmitir o gestionar información de manera digital.

2.11 **RedUCR:** Red telemática institucional que brinda el transporte y acceso IP a los diferentes servicios de la UCR.

2.12 **SSH (Secure Shell):** Protocolo de red criptográfico que permite el acceso remoto seguro para controlar sistemas y transferir archivos a través de redes no seguras como Internet.

2.13 **Usuario remoto:** persona funcionaria, estudiante, docente o externo a la UCR que tenga asignado un permiso de uso del acceso remoto.

2.14 **UCR:** Universidad de Costa Rica.

2.15 **Zoom:** es un servicio de videoconferencia basado en la nube que permite reunirse virtualmente con otras personas.

3. LEYES, REGLAMENTOS O DOCUMENTOS DE REFERENCIA

3.1. La directriz MICITT-DGDCFD-DRII-OF-0011-2024 del Ministerio de Ciencia, Tecnología, Innovación y Telecomunicaciones, establece las medidas son de carácter obligatorio, que incluye acceso remoto, privilegios mínimos entre otros.

3.2. El reglamento vigente del Centro de Informática, en el Artículo 2: inciso 3 indica: “Emitir lineamientos, directrices, estándares y normas, acorde con el área de competencia, según lo que establece el Reglamento de Oficinas Administrativas”. Además; en el inciso 4 indica: “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”.

4. LINEAMIENTOS

4.1. El acceso remoto permite a los usuarios acceder a los recursos desde una ubicación fuera de la RedUCR. Esto es una facilidad y no un derecho que aplica a quienes trabajan desde casa, viajan o necesitan acceder a servicios, archivos o aplicaciones que no están disponibles en su dispositivo local. El acceso remoto es una facilidad restringida ya que, puede ser un vector de ataque y una puerta de entrada que podría comprometer los recursos y servicios institucionales.

4.2. En atención a las directrices del MICITT se recuerdan las medidas obligatorias que hacen referencia al acceso remoto:

4.2.1 Los servicios de correo y VPN deben contar con doble factor de autenticación. Se recomienda evaluar aplicaciones de doble factor como Gaudi, Google authenticator, Microsoft authenticator entre otros, según la necesidad institucional.

4.2.2 Limitar las conexiones VPN solo de acceso desde Costa Rica por geolocalización. Solo bajo circunstancias especiales o por necesidades institucionales, se permitirán accesos desde otros países, siempre con el mínimo privilegio de acceso.

4.2.3 Los usuarios deben cambiar al menos cada 3 meses sus contraseñas. Estas deben ser robustas, con símbolos especiales, alfanumérica con al menos 12 caracteres.

4.2.4. Mantener actualizados los equipos de TI. Deben ejecutar las actualizaciones de forma periódica al menos cada 3 meses. Es necesario que las plataformas cuenten con los parches de seguridad para reducir riesgos de brechas de seguridad.

4.2.5. No deben tener sistemas operativos fuera del soporte del fabricante. Ejemplo: Windows server 2008, 2012, Windows XP, etc. Por lo tanto, es necesario revisar periódicamente las versiones y mantener un control de inventario de los sistemas operativos, así como de las fechas de finalización de su soporte. Esto es fundamental para mantener los sistemas actualizados y dentro del soporte del fabricante, permitiendo así ajustar los planes de migración de las versiones de los sistemas operativos antes de que se vuelvan obsoletos.

4.3. El mecanismo de acceso remoto Institucional se rige por las siguientes condiciones establecidas por el CI:

4.3.1. El servicio de acceso remoto se encuentra deshabitado en la RedUCR por motivos de seguridad de la información, tanto de la institución como de las personas usuarias, se ha establecido una política de control de aplicaciones y protocolos permitidos para fortalecer la ciberseguridad por medio de listas blancas.

4.3.2. Este lineamiento impide el uso de aplicaciones que generen, sin autorización, telemetría, exfiltración de datos y otras situaciones que puedan comprometer la

seguridad institucional como en este caso el compartir escritorios remotos (RDP) por medio de software o similares como AnyDesk o TeamViewer.

4.3.3. Los dispositivos que podrán acceder a la RedUCR deben estar debidamente actualizados, contar con un usuario vigente y autorizado para acceso remoto, tener instalado o conectado a un antivirus, así como, el software de conexión remota de VPN autorizado por CI.

4.3.4. Sólo los usuarios activos a nivel institucional podrán tener derecho a utilizar conexiones de acceso remoto.

4.3.5. No se permite el uso compartido de credenciales (usuario y contraseña) para establecer el acceso remoto.

4.3.6. Los proveedores, contratistas y otros externos a la RedUCR no tendrán derecho a la facilidad de acceso remoto salvo excepciones especiales y autorizadas por el CI.

4.3.7. Los Gestores de TI (GTI) deben velar por el control adecuado de los privilegios de acceso a los recursos a su cargo, producto del establecimiento de la conexión remota.

4.3.8. Las personas teletrabajadoras tienen la responsabilidad de activar los mecanismos de seguridad y actualizaciones necesarias para garantizar la protección de los recursos cuando establezcan una conexión de acceso remoto. Así como, de hacer uso del software de VPN para acceso a la RedUCR y el antivirus institucional facilitado por el CI.

4.3.9. Los dispositivos móviles (institucionales) o personales (BYOD) podrán ser utilizados para establecer conexiones de acceso remoto tomando las medidas de seguridad necesarias. El usuario asume la responsabilidad de la seguridad de esa conexión.

4.3.10. Se debe evitar establecer conexiones desde redes inalámbricas abiertas y en caso de emergencia o fuerza mayor debe recurrir a una conexión de VPN institucional.

4.4. Las conexiones de acceso remoto autorizadas para acceder recursos como red, aplicaciones, archivos y otros se realizarán por medio la habilitación de una sesión remota de MS Teams o Zoom, ambas plataformas con licenciamiento institucional, siempre y cuando el sistema operativo tanto del equipo remoto, como el local cuenten con las más recientes actualizaciones de seguridad y el sistema operativo este soportado por el fabricante. No se permitirá otros mecanismos por seguridad.

4.4.1. Los requisitos de seguridad para el acceso remoto incluyen el uso de una conexión VPN, una validación de MFA y contraseñas seguras entre otros.

4.4.2. El CI está habilitado para bloquear el acceso remoto a direcciones IP que se hayan asociado con actividades maliciosas.

4.4.3. La Institución mantiene el bloqueado del acceso remoto desde países cuya evidencia demuestra que representan un alto riesgo de seguridad.

4.4.4. El CI cuenta con protocolos de respuesta a incidentes de seguridad relacionados con el acceso remoto para atención de eventos asociados.

4.5. La configuración de seguridad para el acceso remoto, como el uso de firewalls, políticas de contraseñas, entre otros deben estar alineados a las pautas de los lineamientos de seguridad emitidos por CI.

4.6. La UCR se reserva el derecho de hacer pruebas de seguridad del acceso remoto para identificar y corregir vulnerabilidades.

4.7. Se suspenderá al usuario el acceso remoto durante un período determinado cuando se haga un uso inapropiado, incumpla las normas de conducta o comprometa la seguridad Institucional en ocasión de este servicio.

5. APROBACIÓN

Actividad	Responsable
Elaboración	M.Sc. Abel Brenes Arce, Coordinador Unidad de Riesgos y Seguridad (URS)
Colaboración	Máster Luis Loría Chavarría, Colaborador URS Lic. Erwin Obregón Aguilera, Colaborador URS Máster Fabiola Rodríguez Alfaro, Colaboradora URS M.Sc. Rebeca Esquivel Flores, Coordinadora Área de Gestión de Comunicaciones (AGC)
Revisión y control	Ing. Jeffrey Dimarco Fernández, Coordinador Unidad de Calidad y Mejora continua (UCM)
Aprobación	Máster Tatiana Bermúdez Páez, Jefe Centro de Informática

UCR Firmado digitalmente