1. PROPÓSITO

Establecer el lineamiento que regula el uso de los dispositivos móviles y dispositivos personales para conexión a recursos de la Universidad de Costa Rica, y es de acatamiento obligatorio para la comunidad universitaria.

2. TÉRMINOS Y ABREVIATURAS

- **AURI:** (Acceso Universitario a la Red Inalámbrica)**.** Plataforma institucional de acceso inalámbrico a RedUCR.
- **Autoridad universitaria responsable:** Persona autorizada para solicitar, administrar y delegar el dominio asignado y subdominios derivados.
- **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.
- **Jailbreaking**: es el proceso de explotar los defectos de un dispositivo electrónico bloqueado para instalar software distinto al que el fabricante ha puesto a disposición del dispositivo
- **CI:** Centro de Informática.
- **Comunidad universitaria**. Está constituida por investigadores, docentes, estudiantes y administrativos de la UCR.
- **Dispositivo móvil:** un equipo electrónico portátil que se puede conectar a Internet, especialmente un teléfono inteligente o una tableta.
- **MDM (Mobile Device Management):** La gestión de dispositivos móviles.
- **NAC (Network Access Control)**: El control de acceso a la red permite controlar qué dispositivos móviles y BYOD pueden acceder a la red de una organización y bajo que esquema de seguridad y calidad de servicio; esto de acuerdo con una postura o política de aseguramiento de los dispositivos versus los recursos por acceder.
- **RedUCR:** Red Telemática Institucional que permite el transporte e integración de las sedes, recintos y otras redes cableadas a las Internet e intranet.
- **Usuario**: corresponde a los funcionarios, docentes o estudiantes de la comunidad universitaria que utilizan dispositivos móviles, dispositivos BYOD o ambos.
- **UCR**: Universidad de Costa Rica.

3. LEYES, REGLAMENTOS O DOCUMENTOS DE REFERENCIA

3.1. El "Reglamento General de las Oficinas Administrativas", de la Universidad de Costa Rica, en su Capítulo III, Artículo 9 inciso f indica: "Emitir directrices, supervisar y establecer procedimientos de acatamiento obligatorio, propias de su área de competencia". Además; en el artículo 10 inciso "o" indica: Establecer, en conjunto con el Consejo Técnico Asesor, las directrices propias del quehacer y prioridad de la oficina a su cargo".

3.2. El reglamento vigente del Centro de Informática establece en el Artículo 2: inciso3 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

Con base en los reglamentos, normas y consideraciones técnicas anteriores, el Centro de Informática determina y emite los siguientes lineamientos generales para el uso de dispositivos móviles.

4.1. Este lineamiento permite a los usuarios utilizar sus propios dispositivos personales, como teléfonos inteligentes, computadoras portátiles y tabletas, para realizar tareas de forma flexible y colaborativa, a esto se le denomina BYOD.

4.2. Se busca proteger la naturaleza crítica de las operaciones de TI ante el uso de dispositivos móviles, así como, a la Institución en el caso de una violación de estas normas.

4.3. Los usuarios que en el desarrollo laboral necesiten utilizar dispositivos móviles institucionales o dispositivos BYOD, son directamente responsables de la información y el acceso a estos elementos.

4.3. La gestión de dispositivos móviles (MDM) será responsabilidad del CI así como, la aplicación de controles y medidas de seguridad, así como llevar el inventario de los dispositivos móviles adquiridos por la Institución. Además, tiene la responsabilidad de implementar tecnologías para el control de acceso a red (NAC) para evitar posibles incidentes de seguridad.

4.4. La adquisición de dispositivos móviles institucionales se realizará en apego a los estándares definidos por el CI y estarán de igual forma bajo estos lineamientos.

5. Dispositivos móviles

5.1. Uso de dispositivos móviles

5.1.1. El usuario deberá solicitar su credencial institucional para integrarse a las plataformas institucionales tales como, red inalámbrica AURI, red cableada RedUCR, servicios en nube, portal universitario entre otros.

5.1.2. El usuario debe validar que la contraseña guardada en el dispositivo móvil asignado o el BYOD estén cifradas, para evitar el acceso a la información e implementar un sistema de contraseñas de 2 o más factores que nos permita un sistema más robusto y seguro.

5.1.3. El usuario debe garantizar que las aplicaciones instaladas en el dispositivo móvil cumplen las listas blancas y negras autorizadas por el CI.

5.1.4. El usuario debe evitar la instalación de aplicaciones en el dispositivo móvil que pueden suponer un peligro para la organización, tales como, las que podrían acceder a información que se exceda de la necesaria para su desarrollo, así como instalar algún tipo de malware.

5.1.5. Se autoriza al usuario a instalar programas o aplicaciones recomendados por el CI en los dispositivos móviles institucionales y sus dispositivos BYOD para el desarrollo de sus actividades laborales.

5.1.6. No se autoriza la instalación de programas de monitoreo o inspección de red y sistemas en los dispositivos móviles o BYOD que se conecten a la RedUCR.

5.1.7. El acceso a recursos y servicios institucionales desde dispositivos móviles debe tener habilitadas medidas de seguridad como la autenticación multifactor y el bloqueo de pantallas entre otras.

5.1.8. No está permitido almacenar información personal ni asociar ningún servicio de uso personal en los dispositivos móviles institucionales.

5.1.9. Los dispositivos móviles en general que hayan pasado por procedimientos de rooteo o “jailbreaking” quedarán prohibidos para ser utilizados en la RedUCR en cualquier forma que impacte o comprometa la seguridad.

5.1.10. El dispositivo móvil o BYOD deberá contar con una adecuada y oportuna gestión de parches, vulnerabilidades y actualizaciones de las aplicaciones, así como del sistema operativo.

5.2. Gestión de dispositivos móviles

Los usuarios de dispositivos móviles, dispositivos BYOD o ambos deben atender los siguientes aspectos cuando accedan la RedUCR dentro o fuera del campus:

5.2.1. Todo dispositivo móvil sin excepción debe tener configurado el bloqueo de pantalla por contraseña y activar un bloqueo durante un periodo de tiempo de al menos 10 minutos en caso de intentos fallidos; todo con el fin de no comprometer la confidencialidad, integridad y disponibilidad de la información contenida en el dispositivo, así como acciones en contra de la RedUCR y sus recursos por parte de terceros.

5.2.2. Limitar el uso de aplicaciones y generar perfiles de acceso con restricción de permisos para evitar la instalación de archivos de origen desconocido.

5.2.3. Actualización de los parches de seguridad y del sistema operativo de manera regular.

5.2.4. Es indispensable la utilización de antivirus actualizado en el dispositivo móvil.

5.2.5. No se autoriza cargar el dispositivo móvil a través de los computadores de la institución.

5.2.6. Utilizar conexiones seguras tipo VPN institucionales que permita activar el sistema de intrusión de amenazas.

5.2.7. Evitar conexión a redes inalámbricas abiertas, tanto dentro como fuera de la institución, esto con el propósito de evitar robo o pérdida de credenciales e información, ya que, este tipo de redes son consideradas técnicamente inseguras.

5.2.8. Cuando el dispositivo BYOD sea utilizado por terceros ajenos a la relación laboral o académica, el usuario debe aumentar los niveles de seguridad para garantizar que no tendrán acceso a ninguna información de la organización que pueda ocasionar un uso fraudulento o indebido de la misma. Así como revisar el estado del dispositivo después del uso, identificando cambios en el mismo tanto a nivel de aplicaciones como de configuración.

5.3. Gestión de dispositivos móviles institucionales

En adición al punto 5.2, en la gestión de dispositivos móviles instituciones se debe considerar:

5.3.1. El dispositivo móvil institucional debe contar con el antivirus institucional y un mecanismo de respaldo y recuperación de información asociado.

5.3.2. Toda la información almacenada en los dispositivos móviles institucionales permanecerá cifrada para evitar accesos no autorizados.

5.3.3. Cuando un dispositivo móvil institucional se pierda o sea robado, el funcionario a cargo debe reportar de inmediato al CI la situación y seguir el procedimiento institucional correspondiente.

5.3.4. No se permite utilizar aplicaciones o ingreso a sitios web para uso personal en los dispositivos móviles institucionales. Igualmente, sitios o aplicaciones web de dudosa procedencia, con contenido inapropiado o que atente contra los fines de la institución serán restringidos.

5.3.5. Los funcionarios aprobados para emplear dispositivos móviles institucionales son directamente responsables de la información institucional y accesos ejecutados, así como el uso adecuado del dispositivo.

5.3.6. Se prohíbe aplicar procedimientos de rooteo (jailbreaking) en los dispositivos móviles institucionales.

5.4. Destrucción de información

El usuario de dispositivos BYOD debe establecer el proceso de destrucción o borrado de información de estos dispositivos cuando cesa la relación laboral.

5.5. Contenido de los dispositivos móviles

5.5.1 El usuario debe proteger a la Institución de no mantener contenido malicioso, materiales ilícitos en sus dispositivos móviles, BYOD o ambos, con información que pueda ser propiedad de otras entidades y afines.

5.5.2 Se recomienda evitar el acceso a sitios o aplicaciones web de dudosa procedencia, con contenido inapropiado o confuso, ya que el riesgo de pérdida o robo de información puede ser mayor.

5.6. Cumplimiento

El incumplimiento de las disposiciones establecidas en este lineamiento puede resultar en la cancelación o suspensión del acceso del dispositivo a la RedUCR y la imposición de sanciones adicionales, de acuerdo con las políticas y regulaciones establecidas por la UCR según el caso.

La UCR se reserva el derecho de revocar un dispositivo móvil, BOYD o ambos si el usuario responsable del dispositivo incumple cualquiera de los términos de este lineamiento.

5.7. Revisión del lineamiento

El presente lineamiento será revisado y actualizado periódicamente, de acuerdo con los cambios en las políticas y regulaciones de la UCR, así como con los avances tecnológicos y las necesidades institucionales.

6. APROBACIÓN

Actividad	Responsable
Elaboración	M.Sc. Abel Brenes Arce, Coordinador Unidad de Riesgos y Seguridad (URS)
Colaboración	Magíster Luis Gmo. Loría Chavarría, colaborador URS
Revisión	Ing. Jeffrey Dimarco Fernández, Coordinador Unidad de Calidad y Mejora Continua (UCM)
Aprobación	Máster Tatiana Bermúdez Páez, Subdirectora CI Bach. Cindy Arias Quiel, Coordinadora Área de Gestión de Adquisiciones (AGA) M.Sc. Abel Brenes Arce, Coordinador URS Lic. Jorge Carranza Chaves, Coordinador Área de Gestión de Infraestructura (AGI) Ing. Javier Vega Ruiz, Coordinador Área de Desarrollo de Servicios (ADS) Ing. Jeffrey Dimarco Fernández, Coordinador UCM) M.Sc. Rebeca Esquivel Flores, Coordinadora Área de Gestión de Comunicaciones (AGC) Ing. Wilfredo Fonseca Vargas, Coordinador Área de Gestión de Servicios (AGS) Lic. Jairo Sosa Mesen, Coordinador Área de Gestión de Usuarios (AGU) Máster Ana Yanci Tosso, Coordinadora Unidad Administrativa y Recurso Humano (UAR) Dr. Henry Lizano, Director CI

UCR Firmado digitalmente