1. PROPÓSITO

Establecer los lineamientos técnicos para la administración efectiva de usuarios, roles y privilegios en sistemas, plataformas y aplicativos institucionales propios o relacionados con las condiciones para garantizar la salvaguarda y funcionamiento de los recursos institucionales, y que deberán ser de acatamiento obligatorio por parte de la comunidad universitaria. Este lineamiento está dirigido a los Gestores de Tecnologías de Información, personal técnico y a la comunidad universitaria.

2. TÉRMINOS Y ABREVIATURAS

- **CI:** Centro de Informática.
- **Gestor de Tecnologías de Información (GTI):** Administrador del Recursos Informático Institucional.
- **Sistemas y aplicativos:** incluye sistemas operativos de servidores y estaciones de trabajo, plataformas, bases de datos, manejadores de contenido, servicios en nube y afines.
- **Usuario administrador (Administrador)**: Encargado de la gestión del sistema o plataforma informática incluyendo la administración de los usuarios. Cuenta con permisos para instalar y mantener software, modificar configuraciones del sistema y gestionar los usuarios a cargo.
- **Usuario estándar**: Desarrolla sus actividades a partir del software instalado y no podrán modificar las configuraciones del sistema.
- **Usuario invitado**: Desarrolla sus actividades a partir del software instalado; su permanencia en el sistema es temporal.
- **Usuario con permisos especiales**: Cuenta con roles y privilegios especiales previamente autorizados para acceso a las plataformas; debe respetar la configuración del sistema y/o plataforma apegándose sólo a las tareas asignadas.
- **UCR:** Universidad de Costa Rica.

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:

  > "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:

  > c). Emitir lineamientos, directrices, estándares y normas, acorde con el área de competencia, según lo que establece el *Reglamento de Oficinas Administrativas*.

d). 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.

- Sobre la responsabilidad de las jefaturas de informar:
  - Las jefaturas deben informar sobre los movimientos de personal (movimientos a otras unidades de trabajo, pensión, procesos administrativos, permisos sin goce, despidos) a los administradores de sistemas, para que cuenten con información oportuna y puedan realizar los cambios o eliminación de cuentas o roles cuando corresponda.

4. LINEAMIENTOS

4.1 El usuario administrador desarrolla actividades críticas de gestión y seguridad sobre plataformas o sistemas a su cargo. Por lo que es importante establecer políticas claras para garantizar que la seguridad y el acceso sea adecuado, restringido y limitado sólo a aquellos que lo requieren según su cargo y responsabilidades para la realización de tareas de acuerdo a su rol institucional.

4.2 El lineamiento define políticas para mejorar la seguridad de los perfiles y accesos, así como la gestión de los sistemas y plataformas, evitando problemas como el ingreso no autorizado a plataformas, sistemas, datos confidenciales, así como, la modificación no autorizada de configuraciones del sistema y la instalación de software no licenciado o malintencionado.

4.3. Lineamientos técnicos para las cuentas de usuarios:

a. Los usuarios que utilicen los servicios informáticos propios o relacionados con la institución se clasifican principalmente de acuerdo con los siguientes roles:
   - Administrador
   - Usuario estándar
   - Usuario invitado
   - Usuario con permisos especiales

b. Todos los usuarios deben establecer robustas contraseñas (passwords), esto según los lineamientos específicos y las facilidades de los sistemas y plataformas, donde preferiblemente utilizar al menos una longitud de doce en combinaciones de letras, dígitos y símbolos.

c. Los usuarios deberán cambiar la contraseña conforme al formato indicado y a la frecuencia establecida por el usuario administrador o el lineamiento vigente.

d. La Institución se reserva el derecho de remover o suspender usuarios de forma temporal o permanente cuando dejen de utilizar el servicio por motivos tales como, pero sin limitarse a, jubilación, renuncia, cambio de trabajo u otros motivos que afecten su capacidad o interés en utilizar el servicio y accesos.

4.4 Lineamientos técnicos de cuentas de usuario administrador:

a. El administrador es aquel que tiene acceso a los sistemas y recursos con niveles de privilegio que permiten la realización de cambios críticos o de impacto en la

configuración del sistema, que incluye la instalación de software o componentes, gestión de cuentas de usuario, entre otros.

b. El administrador es responsable de la gestión y mantenimiento de usuarios (creación, modificación, suspensión y borrado de cuentas) así como la asignación de los roles correspondientes a cada clasificación de usuarios. También es el responsable de administrar otros roles permitidos en las plataformas que gestiona, en casos como, los manejadores de contenido o sistemas de gestión de base de datos.

c. Cuando un usuario requiera la clasificación de usuario con permisos especiales deberá elevar su solicitud por escrito ante la jefatura de la oficina o unidad, justificando las excepciones para contar con roles o privilegios sobre el resto de los usuarios del sistema o plataforma. En caso de aprobación de la solicitud, el Administrador procederá de conformidad.

4.5 La gestión del usuario administrador establece, pero no se limita a lo siguiente:

a. Tendrá acceso a todas las funciones del sistema o plataforma y la gestión asociada de usuarios que incluye la creación, modificación, suspensión, borrador.

b. Establecerá las políticas de privilegios para cada tipo y/o grupo de usuarios.

c. Sólo personal calificado será autorizado para contar con acceso tipo administrador en los diferentes sistemas y plataformas: sistemas operativos, dispositivos de red, bases de datos, aplicativos en nube, desarrolladores de software y a otras labores técnicas.

d. Configurar las políticas de las contraseñas de los usuarios conforme al lineamiento respectivo en cada sistema, plataforma o aplicativo a cargo.

e. Debe realizar un seguimiento continuo de las políticas de privilegios y accesos para asegurarse de que estén actualizadas y se ajusten a las necesidades del sistema.

f. Debe implementar herramientas de gestión de usuarios y roles para facilitar la administración del sistema y el monitoreo de los mismos

4.6 La asignación, competencias, renovación y trazabilidad del usuario administrador:

a. El acceso al usuario administrador debe ser asignado sólo después de una verificación de antecedentes adecuada y una evaluación de la necesidad del acceso.

b. La persona usuaria administrador debe contar con las competencias necesarias para el desempeño de sus labores y aplicar los lineamientos y procedimientos de seguridad institucional en todo momento.

c. El usuario administrador debe ser revocado inmediatamente cuando ya no sea necesario o cuando se produzca una violación de la seguridad. El proceso de revocación de acceso debe ser divulgado de preaviso y bien documentado.

d. Se debe contar con bitácoras de las actividades en el sistema, incluso la del administrador. Los registros deben estar disponibles para ser auditados en búsqueda de intentos de acceso no autorizados o actividades sospechosas.

e. El usuario administrador es intransferible, excepto cuando haya cambio de una persona administradora a otra.

Este lineamiento está dirigido a los Gestores de Tecnologías de Información, personal técnico y a la comunidad universitaria.

5. APROBACIÓN

Actividad	Responsable
Elaboración	M.Sc. Abel Brenes Arce, Coordinador Unidad de Riesgos y Seguridad (URS)
Colaboración	M.Sc. Luis Loría Chavarría, Colaborador URS M.B.A. Jesús Brenes Fernández, Colaborador URS
Revisión	Ing. Jeffrey Dimarco, Coordinador Unidad de Calidad y Mejora Continua (UCM)
Aprobación	Dr. Henry Lizano, Director C.I.

UCR Firmado digitalmente